
GAZİ ÜNİVERSİTESİ
Gazi
1926

DİJİTAL DÖNÜŞÜM İÇİN BLOKZİNCİR KULLANIMINA YÖNELİK BİR KARAR VERME MODELİ ÖNERİSİ: KAMU İHALE SÜRECİ UYGULAMA ÖRNEĞİ

Çetin KARAHAN

DOKTORA TEZİ
YÖNETİM BİLİŞİM SİSTEMLERİ ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

OCAK 2023

Çetin KARAHAN tarafından hazırlanan "DİJİTAL DÖNÜŞÜM İÇİN BLOKZİNCİR KULLANIMINA YÖNELİK BİR KARAR VERME MODELİ ÖNERİSİ: KAMU İHALE SÜRECİ UYGULAMA ÖRNEĞİ" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi Yönetim Bilişim Sistemleri Ana Bilim Dalında DOKTORA TEZİ olarak kabul edilmiştir.

Danışman: Prof. Dr. Aslıhan TÜFEKCİ

Yönetim Bilişim Sistemleri Ana Bilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum.

Başkan: Prof. Dr. Hacer KARACAN

Bilgisayar Mühendisliği Bölümü, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum.

Üye: Doç. Dr. Gökhan ŞENGÜL

Bilgisayar Mühendisliği Bölümü, Atılım Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum.

Üye: Doç. Dr. Murat YILMAZ

Bilgisayar Mühendisliği Bölümü, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum.

Üye: Prof. Dr. Muzaffer KAPANOĞLU

Endüstri Mühendisliği Bölümü, Eskişehir Osmangazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Doktora Tezi olduğunu onaylıyorum.

Tez Savunma Tarihi: 16/01/2023

Jüri tarafından kabul edilen bu tezin Doktora Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

Prof. Dr. Aslıhan TÜFEKCİ

Bilişim Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Bilişim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Çetin KARAHAN

16/01/2023

DİJİTAL DÖNÜŞÜM İÇİN BLOKZİNCİR KULLANIMINA YÖNELİK BİR KARAR VERME MODELİ ÖNERİSİ: KAMU İHALE SÜRECİ UYGULAMA ÖRNEĞİ

(Doktora Tezi)

Çetin KARAHAN

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Ocak 2023

ÖZET

Kamu hizmetlerinin elektronik ortamda sunulmasını ifade eden e-devlet yerini artık hizmetleri ve süreçleri yeniden tasarlamayı gerektiren dijital devlet kavramına bırakmıştır. Dijital devletin temelinde değer yaratmak, üretkenliği ve sosyal refahı artırmak için özellikle yenilikçi teknolojilerin kullanılmasıyla ifade edilen dijital dönüşüm yatmaktadır. Verilerin değiştirilememesi, aracıların devre dışı bırakılması, şeffaflık gibi avantajlar sunan benzersiz yapısıyla blokzincir bu yenilikçi teknolojilerden en önemlilerinden biri olup ortaya ilk çıktığı 2008 yılından günümüze sürekli uygulama alanı genişleyen ve avantajlarından faydalanmak için üzerinde çalışılmaya hâlâ devam edilen bir teknolojidir. Teknik yapısı ve özelliklerinin karmaşıklığı, farklı yönetişim anlayışı ve çok sayıda alternatif blokzincir platformunun bulunması gibi nedenler bu teknolojinin özellikle kamu sektöründe kullanım kararının verilmesini ve gerçek hayat uygulamalarının geliştirilmesini güçleştirmektedir. Dijital anlamda gelişmiş devletlerde bu teknolojinin uygulanmasına yönelik çalışmalar uzun zaman önce başlamış, dijital kimlik, seçimler, tapu kaydı gibi kamu hizmetlerinde kullanımına yönelik prototiplerle gerçek dünya uygulamalarında denenmeye başlanmıştır. Türkiye kamu sektöründe ise henüz blokzincirin kullanımına yönelik bir örnek bulunmamaktadır. Bu tez çalışmasında, dünya örnekleri de dikkate alınarak, blokzincirin kamu sektöründe kullanımı için ülkemizin hazır bulunuşluk durumu analiz edilerek kullanımı kararı ile bu karar sonrası geliştirilecek tasarıma ilişkin konularda kamu sektörü karar vericilerinin kararlarına destek sağlayacak bir model geliştirilmiştir. Model kapsamında özellikleri, avantajları, kısıtlılıkları ve kullanım alanları analiz edilerek blokzincirin kullanılabilir olup olmadığı çıktısını sunan karar listeleri ve karar ağacı oluşturulmuştur. En uygun blokzincir çözümünü belirlemek için kriterler, bunların öncelikleri ve alternatiflerin bir arada değerlendirilmesi işlemlerini içeren Çok Kriterli Karar Verme durumu için Analitik Hiyerarşi Prosesi kullanılmıştır. Model ile, kullanım kararı ve en uygun çözüm alternatifine ilişkin bir karar destek sistemi önerilmektedir. Modele esas teşkil eden form, liste ve çizelgeler bir şablon olarak hazırlanmış olup bu hali ile model, girdilerinde değişiklik, güncelleme ve ilave yapılmasına, yeni platform eklenmesine uygun, gelecekte gerçekleşecek gelişmeler, ortaya çıkacak yeni platformlar ve farklı seçim kriterlerine göre genişletilebilir bir yapıdadır.

Bilim Kodu	:	114606
Anahtar Kelimeler	:	Blokzincir, blokzincir platformu, çok kriterli karar verme, analitik hiyerarşi prosesi, dijital dönüşüm
Sayfa Adedi	:	393
Danışman	:	Prof. Dr. Aslıhan TÜFEKCİ

A DECISION-MAKING MODEL PROPOSAL TO USE BLOCKCHAIN FOR DIGITAL TRANSFORMATION: PUBLIC TENDERING PROCESS USE CASE

(Ph. D. Thesis)

Çetin KARAHAN

GAZİ UNIVERSITY

INSTITUTE OF INFORMATICS

January 2023

ABSTRACT

E-government, which indicates the provision of public services in electronic environment, has now been replaced by digital government concept which requires redesigning services and processes. Digital transformation, which depicts using disruptive technologies for creating value, increasing productivity, and social welfare, underlies this digital government concept. With its unique structure that offers advantages such as immutability, eliminating intermediaries, and transparency, blockchain is one of the most important of these disruptive technologies. It has ever-expanding use cases and has been still studied on to take advantage of its strengths since its first appearance in 2008. The reasons such as complexity of its technical specifications, unconventional governance structure, and the existence of many alternative blockchain platforms make it difficult to decide on the use of this technology and hinder the development of real-life applications, especially in the public sector. Digitally developed countries have been studying this technology for a long time and many of them have already developed prototypes for its use in public services such as digital identity, elections, and land registry for testing blockchain in real-world applications. However, there is no example of the use of blockchain in Turkish public sector yet. In this thesis, the readiness for the use of blockchain in public sector in Turkey has been analyzed and a model that will support the decisions of the public sector decision-makers on the decision to use blockchain technology with its design has been developed. Within the scope of the model, decision lists and decision trees that produce the decision of whether the blockchain is usable or not were created by analysis of the main features, advantages, limitations and use cases. Analytical Hierarchy Process has been used for the Multi-Criteria Decision Making situation, which includes the evaluation of multiple criteria and their priorities together with alternatives to determine the most appropriate solution. With the model, a decision support system is proposed regarding the usage decision and the most suitable solution alternative. The forms, lists and evaluation tables, which form the basis of the model, have been prepared as a template. Hence, the model is suitable for making changes, updates, and additions to the inputs and adding new platforms. It is in an extensible format in accordance with future developments, emerging platforms, and possible different selection criteria.

Science Code	:	114606
Key Words	:	Blockchain, blockchain platform, multi-criteria decision-making, analytic hierarchy process, digital transformation
Page Number	:	393
Supervisor	:	Prof. Dr. Aslıhan TÜFEKCİ

TEŞEKKÜR

Doktora tez çalışmam boyunca yönlendirmeleri, hoşgörüsü ve pozitif yaklaşımı ile her anlamda desteğini en derinden hissettiğim, tezin her aşamasında büyük katkı ve emekleri bulunan, hem akademik gelişimime hem de profesyonel hayatıma kattıkları ile her türlü teşekkürün yetersiz kaldığı değerli danışmanım Prof. Dr. Aslıhan TÜFEKCİ'ye sonsuz minnet ve teşekkürlerimi sunuyorum.

Tez izleme komitesinde yer alarak çalışmanın tüm aşamalarında değerli bilgilerini, önerilerini ve zamanlarını esirgemeyen, her zaman yapıcı ve yönlendirici tutumlarıyla süreci kolaylaştıran saygıdeğer hocam Prof. Dr. Hacer KARACAN ve saygıdeğer hocam Doç. Dr. Gökhan ŞENGÜL'e katkıları için teşekkürü bir borç bilirim.

Uzun ve yoğun bir biçimde geçen tez döneminde varlıkları ile her zaman bana moral ve güç veren canım oğlum Baray Taylan KARAHAN ve biricik kızım Alya Gülin KARAHAN'a teşekkür ederim.

Son olarak, eğitim hayatımın en başından beri her türlü fedakârlık, özveri ve maddi-manevi destekleri ile bu çalışmanın ve bu zamana kadar edindiğim tüm diploma ve unvanların asıl sahibi olan sevgili annem Ayşe KARAHAN başta olmak üzere tüm aileme sonsuz teşekkür ederim.

İÇİNDEKİLER

Sayfa

ÖZET iv

ABSTRACT v

TEŞEKKÜR vi

İÇİNDEKİLER vii

KISALTMALAR xxi

1. GİRİŞ 1

2. BLOKZİNCİR TEKNOLOJİSİNİN ÖZELLİKLERİ VE ÇOK KRİTERLİ KARAR VERME 7

2.1. Blokzincir Teknolojisi 7

2.1.1. Blokzincir teknolojisinin tarihçesi 10

2.1.2. Blokzincirin çalışma prensibi – Bitcoin örneği 22

2.1.3. Dağıtık kayıt defteri ve blokzincir teknolojisi 32

2.1.4. Blokzincirde gizlilik ve mahremiyet 33

2.1.5. Blokzincirin potansiyel kullanım alanları ve mevcut uygulamalar 36

2.1.6. Blokzincirin güçlü yönleri ve sunduğu fırsatlar 47

2.1.7. Blokzincirin zayıf yönleri ve tehditler 53

2.1.8. Blokzincir ile merkezi veritabanı karşılaştırması 68

2.1.9. Blokzincir çeşitleri 70

2.1.10. Bizans generalleri problemi ve çifte harcama (Double spending) 73

2.1.11. Mutabakat Mekanizmaları 74

2.1.12. Blokzincir platformları 85

2.1.13. Akıllı sözleşmeler 129

2.2. Standardizasyon ve Yasal Düzenleme Çalışmaları 131

2.2.1. Uluslararası Standardizasyon Teşkilatı (ISO) faaliyetleri 131

2.2.2. Uluslararası Telekomünikasyon Birliği (ITU) faaliyetleri 134

Sayfa

2.2.3. Diğer standardizasyon faaliyetleri 135
2.2.4. Blokzincir ve dağıtık kayıt defteri düzenlemeleri 136
2.3. Uluslararası Kuruluşlar ve Devletlerce Yürütülen Çalışmalar 141
2.3.1. Avrupa Birliği Faaliyetleri 142
2.3.2. Birleşmiş Milletler Faaliyetleri 145
2.3.3. Devletler tarafından yürütülen faaliyetler 148
2.4. Türkiye'de Blokzincir Çalışmaları 154
2.4.1. Türkiye'de blokzincir ekosistemi 154
2.4.2. Mevcut düzenleme faaliyetleri 156
2.5. Türkiye Kamu Sektörü Hizmetleri ve Blokzincir Kullanım Potansiyeli 162
2.5.1. e-Devlet kapısında sunulan hizmetler 164
2.6. Blokzincirin Kullanılabilirliğinin Değerlendirmesi İçin Karar Modelleri 169
2.7. Çok Kriterli Karar Verme (ÇKKV) Metotları 177
2.7.1. Ağırlıklandırılmış Toplam Modeli (The Weighted Sum Model) 178
2.7.2. Ağırlıklandırılmış Çarpım Modeli (The Weighted Product Model) 181
2.7.3. Analitik Hiyerarşi Prosesi (The Analytic Hierarchy Process) 182
2.7.4. Revize Edilmiş Analitik Hiyerarşi Prosesi (The Revised Analytic Hierarchy Process) 200
2.7.5. Bulanık Analitik Hiyerarşi Prosesi (The Fuzzy Analytic Hierarchy Process) 201
2.7.6. ELECTRE (Elimination et Choix Traduisant La Realite) Metodu 202
2.7.7. TOPSIS (Technique for Order of Preference by Similarity to Ideal Solution) Metodu 211
2.7.8. Çok Kriterli Karar Verme metotlarının karşılaştırılması 215
3. YÖNTEM 217
4. BLOKZİNCİR TEKNOLOJİSİNİN KULLANIMI İÇİN BİR MODEL ÖNERİSİ 225
4.1. Model İşlem Adımları 226

Sayfa

4.1.1. Adım 1. Bilgi Tabanı 226

4.1.2. Adım 2. Kural Tabanı 242

4.1.3. Adım 3. Süreç seçimi, bilgi toplama ve veri girişi 251

4.1.4. Adım 4. Hesaplama motoru 256

4.1.5. Adım 5. Teknoloji seçimi ve sistem tasarımı 260

5. BLOKZİNCİR TEKNOLOJİSİNİN KULLANILABİLİRLİĞİ VE ÇÖZÜM SEÇİMİ İÇİN BİR UYGULAMA: KAMU İHALE SÜRECİ 263

5.1. Adım 1: Bilgi Tabanı 264

5.2. Adım 2: Kural Tabanı 265

5.3. Adım 3. Süreç Seçimi, Bilgi Toplama ve Veri Girişi 265

5.4. Adım 4. Hesaplama Motoru 273

5.4.1. Blokzincir teknolojisinin seçilen süreç veya senaryo için uygun çözüm olup olmadığına karar verilmesi 273

5.4.2. Uygun blokzincir çözümünün özelliklerinin, karar vermek için gerekli kriterlerin ve çözüm alternatiflerinin belirlenmesi 276

5.4.3. Çözüm alternatiflerinin bu özelliklere göre değerlendirilerek öncelik sırasına göre sıralanması 311

5.5. Adım 5. Teknoloji Seçimi ve Sistem Tasarımı 313

5.5.1. Sürecin blokzincir kullanımına uygun biçimde tasarlanması 313

5.5.2. Öncelik sırasına göre ilk sıradaki platformun özellikleri 340

6. SONUÇ VE ÖNERİLER 347

KAYNAKLAR 353

EKLER 377

EK-1. Süreç Bilgi Formu 378

EK-2. Süreç Bilgi Formu (Kamu İhale Süreci) 383

ÖZGEÇMİŞ 391

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

Çizelge 2.1. Bitcoin sistemindeki blok içeriği 27

Çizelge 2.2. Bitcoin blok başlığının içerdiği veriler 27

Çizelge 2.3. Blokzincir teknolojisinin başlıca kullanım alanları 46

Çizelge 2.4. GDPR veri sahibi haklarının blokzincir kapsamında analizi (Finck, 2018) 55

Çizelge 2.5. Blokzincir ile veri tabanının temel farkları (Anwar, 2018) 70

Çizelge 2.6. Blokzincir platformlarının özelliklerinin belirlenmesi için değerlendirme şablonu 86

Çizelge 2.7. Bazı blokzincir platformlarının güvenlik ve performans özellikleri 88

Çizelge 2.8. Bitcoin platformunun özellikleri..... 89

Çizelge 2.9. Ethereum platformunun özellikleri..... 92

Çizelge 2.10. Hyperledger platformunun başlıca projelerinin (Fabric, Sawtooth, Iroha, Indy) özellikleri..... 95

Çizelge 2.11. Stellar platformunun özellikleri..... 101

Çizelge 2.12. Quorum platformunun özellikleri..... 103

Çizelge 2.13. Corda platformunun özellikleri..... 104

Çizelge 2.14. MultiChain blokzincir platformunun özellikleri..... 106

Çizelge 2.15. OpenChain blokzincir platformunun özellikleri..... 108

Çizelge 2.16. BigchainDB blokzincir platformunun özellikleri..... 110

Çizelge 2.17. IOTA Tangle platformunun özellikleri..... 113

Çizelge 2.18. HydraChain blokzincir platformunun özellikleri..... 115

Çizelge 2.19. Avalanche blokzincir platformunun özellikleri..... 118

Çizelge 2.20. Parity Substrate blokzincir platformunun özellikleri..... 121

Çizelge 2.21. Kadena blokzincir platformunun özellikleri..... 123

Çizelge 2.22. ISO/TC 307 kapsamında görev yapan araştırma ve çalışma grupları (Ekim 2022)..... 132

Çizelge 2.23. ISO/TC 307 sorumluluğunda yayınlanmış olan standartlar 132

Çizelge 2.24. ISO/TC 307 sorumluluğunda geliştirilmeye devam eden standartlar..... 133

Çizelge **Sayfa**

Çizelge 2.25. ITU-T Dağıtık Kayıt Defteri Teknolojileri Odak Grubu yayınları..... 135

Çizelge 2.26. IEEE tarafından yürütülen standardizasyon çalışmaları (Geliştirme aşamasında olanların tamamı alınmamıştır)..... 135

Çizelge 2.27. Avrupa Birliği ve dünya ülkeleri tarafından yayınlanan düzenleme sayıları 140

Çizelge 2.28. Ülkelere göre yasal düzenleme sayıları 140

Çizelge 2.29. Ülkeler ve uluslararası kuruluşlarca gerçekleştirilmiş olan blokzincir kamu uygulamalarının sayıları 150

Çizelge 2.30. Blokzincir konulu faaliyetlerin konularına göre dağılımları 152

Çizelge 2.31. Dünyadan kamu blokzincir uygulamalarının sektörlere göre sayıları..... 153

Çizelge 2.32. Kamu kurumları tarafından verilen hizmet sayıları (KAYSİS – 29.10.2022)..... 163

Çizelge 2.33. Blokzincirin potansiyel kullanım alanları ve katacağı değer..... 166

Çizelge 2.34. Her bir alternatif için ilgili kriter değerleri ve kriter ağırlıkları – ATM... 179

Çizelge 2.35. Her bir kriter için maksimum ya da minimum değerler – ATM 180

Çizelge 2.36. Normalizasyon işlemi – ATM 180

Çizelge 2.37. Normalize edilmiş karar matrisi – ATM 180

Çizelge 2.38. Her bir kritere göre alternatif değerlerinin ağırlıklarla çarpımı – ATM... 181

Çizelge 2.39. Ağırlıklandırılmış Çarpım Modeli için normalize edilmiş karar matrisi.. 182

Çizelge 2.40. Her bir kritere göre alternatif değerlerinin ağırlıklara göre üsleri – AÇM..182

Çizelge 2.41. AHP için temel ölçek (Saaty R. W., 1987)..... 185

Çizelge 2.42. Farklı yazarlar tarafından hesaplanmış RI değerleri (Alonso ve Lamata, 2006)..... 189

Çizelge 2.43. Blokzincir platform seçim kriterleri ikili karşılaştırma matrisi (AHP uygulama örneği)..... 191

Çizelge 2.44. Normalize edilmiş ikili karşılaştırma matrisi (AHP uygulama örneği).... 192

Çizelge 2.45. Platform özellikleri için tutarlılık analizi değerleri (AHP uygulama örneği) 192

Çizelge 2.46. İşlem hacmi kriterine göre platform alternatiflerinin ikili karşılaştırma matrisi 193

Çizelge **Sayfa**

Çizelge 2.47. Normalize edilmiş ikili karşılaştırma matrisi – İşlem Hacmi (AHP uygulama örneği)..... 194

Çizelge 2.48. Tutarlılık analizi hesaplamalarında kullanılan hesaplama ve formüller (AHP uygulama örneği) 194

Çizelge 2.49. İşlem hacmine göre platform alternatifleri için tutarlılık analizi hesaplamaları (AHP uygulama örneği) 194

Çizelge 2.50. İşlem hızı kriterine göre platform alternatiflerinin ikili karşılaştırma matrisi (AHP uygulama örneği) 195

Çizelge 2.51. Normalize edilmiş ikili karşılaştırma matrisi – İşlem Hızı (AHP uygulama örneği)..... 196

Çizelge 2.52. İşlem hızına göre platform alternatifleri için tutarlılık analizi hesaplamaları (AHP uygulama örneği) 196

Çizelge 2.53. Olgunluk kriterine göre platform alternatiflerinin ikili karşılaştırma matrisi (AHP uygulama örneği) 197

Çizelge 2.54. Normalize edilmiş ikili karşılaştırma matrisi – Olgunluk (AHP uygulama örneği)..... 197

Çizelge 2.55. Olgunluğa göre platform alternatifleri için tutarlılık analizi hesaplamaları (AHP uygulama örneği) 197

Çizelge 2.56. Popülarite kriterine göre platform alternatiflerinin ikili karşılaştırma matrisi (AHP uygulama örneği) 198

Çizelge 2.57. Normalize edilmiş ikili karşılaştırma matrisi – Popülarite (AHP uygulama örneği)..... 198

Çizelge 2.58. Popülariteye göre platform alternatifleri için tutarlılık analizi hesaplamaları (AHP uygulama örneği) 199

Çizelge 2.59. Alternatiflerin ikili karşılaştırmaları sonucunda elde edilen ağırlık vektörleri (AHP uygulama örneği)..... 199

Çizelge 2.60. Bulanık AHP önem tablosu (Rao'dan (2008) uyarlanmıştır) 201

Çizelge 2.61. Blokzincir platformu alternatifleri için ilgili kriter değerleri ve kriter ağırlıkları – ELECTRE metodu..... 203

Çizelge 2.62. Blokzincir platformu alternatifleri için normalize karar matrisi hesaplamaları – ELECTRE metodu 204

Çizelge 2.63. Blokzincir platformu alternatifleri için normalize karar matrisi – ELECTRE metodu 204

Çizelge **Sayfa**

Çizelge 2.64. Blokzincir platformu alternatifleri için ağırlıklı normalize karar matrisi – ELECTRE metodu 205

Çizelge 2.65. Blokzincir platformu alternatifleri için uyum ve uyumsuzluk kümeleri – ELECTRE metodu 206

Çizelge 2.66. Blokzincir platformu alternatifleri için uyum ve uyumsuzluk matrislerinin elemanları – ELECTRE metodu 207

Çizelge 2.67. Blokzincir platformu alternatifleri için uyum matrisi – ELECTRE metodu 207

Çizelge 2.68. Blokzincir platformu alternatifleri için uyumsuzluk matrisi – ELECTRE metodu 208

Çizelge 2.69. Blokzincir platformu alternatifleri için uyum üstünlük matrisi – ELECTRE metodu 209

Çizelge 2.70. Blokzincir platformu alternatifleri için uyumsuzluk üstünlük matrisi – ELECTRE metodu 209

Çizelge 2.71. Blokzincir platformu alternatifleri için baskınlık matrisi – ELECTRE metodu 210

Çizelge 2.72. Blokzincir platformu alternatifleri için nihai baskınlık matrisi – ELECTRE metodu 210

Çizelge 2.73. Blokzincir platformu alternatifleri için ilgili kriter değerleri ve kriter ağırlıkları – TOPSIS metodu 211

Çizelge 2.74. Blokzincir platformu alternatifleri için normalize karar matrisi – TOPSIS metodu 212

Çizelge 2.75. Blokzincir platformu alternatifleri için ağırlıklı normalize karar matrisi – TOPSIS metodu 212

Çizelge 2.76. En iyi ve en kötü alternatif değerleri – TOPSIS metodu 213

Çizelge 2.77. Blokzincir alternatifleri için Öklid mesafeleri – TOPSIS metodu 214

Çizelge 2.78. Blokzincir alternatifleri için performans skorları – TOPSIS metodu 214

Çizelge 2.79. Tüm metotlara göre blokzincir platform alternatiflerinin öncelik sıralaması 215

Çizelge 4.1. Kullanım senaryosu için blokzincir çözümünün uygun olup olmadığı kararında kullanılan sorular 230

Çizelge 4.2. Blokzincir teknolojisinin kullanımının uygun olduğu ve olmadığı durumlar 234

Çizelge **Sayfa**

Çizelge 4.3. Blokzincir teknolojisine ilişkin fonksiyonel ve fonksiyonel olmayan gereksinimler 235

Çizelge 4.4. Blokzincir teknolojisinin avantajları ve güçlü yönleri 235

Çizelge 4.5. Blokzincir teknolojisinin dezavantajları ve zayıf yönleri 237

Çizelge 4.6. Blokzincir teknolojisinin hâlihazırda uygulanabilir olduğu süreçler 238

Çizelge 4.7. Blokzincir platformu karşılaştırma tablosu 240

Çizelge 4.8. Blokzincir platformu karşılaştırma tablosu açıklamaları 241

Çizelge 4.9. Blokzincir platformunun niteliklerine ilişkin seçenekler (kesin özellik) ... 243

Çizelge 4.10. Blokzincir platformunun niteliklerine ilişkin seçenekler (derece belirten) .244

Çizelge 4.11. Blokzincir kullan-kullanma listesi 245

Çizelge 4.12. Blokzincir çözümünün değerlendirilmesinde kullanılan nitelikler 246

Çizelge 4.13. Blokzincir platformları için ikili karşılaştırma nitelikleri 247

Çizelge 4.14. MoSCoW listesine göre platform değerlendirme tablosu 249

Çizelge 4.15. Süreç Bilgi Formu çıktılarının kullanım alanları 252

Çizelge 4.16. Süreç performans parametreleri için maksimum ve minimum değerler .. 253

Çizelge 4.17. Süreç performans parametreleri için eşik değerler 253

Çizelge 4.18. MoSCoW metodu – önceliklerin belirlenmesi için kullanılan seçim listesi 253

Çizelge 4.19. Örnek ikili karşılaştırma matrisi (Model adımı 3) 254

Çizelge 4.20. Örnek ikili karşılaştırma matrisi şablonu (Model adımı 3) 255

Çizelge 5.1. İhale süreci işlem hacmi (yıl/ihale sayısı) 266

Çizelge 5.2. Blokzincir platformunun kesin niteliklerine ilişkin seçenekler (ihale süreci) 268

Çizelge 5.3. Blokzincir platformunun derece belirten niteliklerine ilişkin seçenekler (ihale süreci) 268

Çizelge 5.4. MoSCoW– önceliklerin belirlenmesi için kullanılan seçim listesi (ihale süreci) 269

Çizelge 5.5. Blokzincir platformları için ikili karşılaştırma nitelikleri (ihale süreci) 270

Çizelge **Sayfa**

Çizelge 5.6. Seçim kriterlerinin birbirlerine göre önem dereceleri (ihale süreci) 272

Çizelge 5.7. Hâlihazırdaki blokzincir kullanım alanlarına göre ihale sürecinin değerlendirilmesi 273

Çizelge 5.8. Blokzincir kullanım kararı karar ağacı soru ve yanıtları (ihale süreci) 274

Çizelge 5.9. MoSCoW listesine göre platform değerlendirme tablosu 277

Çizelge 5.10. Seçim kriterleri ikili karşılaştırma matrisi 279

Çizelge 5.11. Normalize edilmiş ikili karşılaştırma matrisi (N) 280

Çizelge 5.12. Öncelik Vektörü – Kriterler arası (Ö) 280

Çizelge 5.13. Seçim kriterleri (platform özellikleri) için tutarlılık analizi değerleri (NxÖ) 281

Çizelge 5.14. Blokzincir platformlarının seçim kriterlerine göre özellikleri 282

Çizelge 5.15. Güvenilirlik kriterine göre alternatiflerin ikili karşılaştırma matrisi 284

Çizelge 5.16. Normalize edilmiş ikili karşılaştırma matrisi - Güvenilirlik (N) 284

Çizelge 5.17. Öncelik Vektörü – Güvenilirlik (Ö) 285

Çizelge 5.18. Tutarlılık analizi tablosu - Güvenilirlik (NxÖ) 285

Çizelge 5.19. Olgunluk kriterine göre alternatiflerin ikili karşılaştırma matrisi 287

Çizelge 5.20. Normalize edilmiş ikili karşılaştırma matrisi - Olgunluk (N) 288

Çizelge 5.21. Öncelik Vektörü – Olgunluk (Ö) 288

Çizelge 5.22. Tutarlılık analizi tablosu - Olgunluk (NxÖ) 289

Çizelge 5.23. Popülarite kriterine göre alternatiflerin ikili karşılaştırma matrisi 290

Çizelge 5.24. Normalize edilmiş ikili karşılaştırma matrisi - Popülarite (N) 291

Çizelge 5.25. Öncelik Vektörü – Popülarite (Ö) 291

Çizelge 5.26. Tutarlılık analizi tablosu – Popülarite (NxÖ) 292

Çizelge 5.27. Öncelik Vektörü – Sybil direnci (Ö) 293

Çizelge 5.28. Tutarlılık analizi tablosu - Sybil Direnci (NxÖ) 293

Çizelge 5.29. Kuantum direnci kriterine göre alternatiflerin ikili karşılaştırma matrisi. 294

Çizelge 5.30. Normalize edilmiş ikili karşılaştırma matrisi - Kuantum direnci (N) 295

Çizelge **Sayfa**

Çizelge 5.31. Öncelik Vektörü – Kuantum direnci (Ö) 295

Çizelge 5.32. Tutarlılık analizi tablosu - Kuantum direnci (NxÖ) 296

Çizelge 5.33. DoS ve DDoS direnci kriterine göre alternatiflerin ikili karşılaştırma matrisi 297

Çizelge 5.34. Normalize edilmiş ikili karşılaştırma matrisi – DoS & DDoS Direnci (N). 298

Çizelge 5.35. Öncelik Vektörü – DoS & DDoS Direnci (Ö) 298

Çizelge 5.36. Tutarlılık analizi tablosu – DoS&DDoS direnci (NxÖ) 299

Çizelge 5.37. Ağ gecikmesi kriterine göre alternatiflerin ikili karşılaştırma matrisi 300

Çizelge 5.38. Normalize edilmiş ikili karşılaştırma matrisi - Ağ gecikmesi (N) 301

Çizelge 5.39. Öncelik Vektörü – Ağ gecikmesi (Ö) 301

Çizelge 5.40. Tutarlılık analizi tablosu – Ağ gecikmesi (NxÖ) 302

Çizelge 5.41. İşlem hacmi kriterine göre alternatiflerin ikili karşılaştırma matrisi 303

Çizelge 5.42. Normalize edilmiş ikili karşılaştırma matrisi - İşlem hacmi (N) 304

Çizelge 5.43. Öncelik Vektörü – İşlem hacmi (Ö) 304

Çizelge 5.44. Tutarlılık analizi tablosu - İşlem hacmi (NxÖ) 305

Çizelge 5.45. İşlem hızı kriterine göre alternatiflerin ikili karşılaştırma matrisi 306

Çizelge 5.46. Normalize edilmiş ikili karşılaştırma matrisi – İşlem hızı (N) 307

Çizelge 5.47. Öncelik Vektörü – İşlem hızı (Ö) 307

Çizelge 5.48. Tutarlılık analizi tablosu - İşlem hızı (NxÖ) 308

Çizelge 5.49. Token kullanımı kriterine göre alternatiflerin ikili karşılaştırma matrisi . 309

Çizelge 5.50. Normalize edilmiş ikili karşılaştırma matrisi - Token kullanımı (N) 310

Çizelge 5.51. Öncelik Vektörü – Token kullanımı (Ö) 310

Çizelge 5.52. Tutarlılık analizi tablosu – Token kullanımı (NxÖ) 311

Çizelge 5.53. Alternatiflerin kriterlere göre karşılaştırma öncelik vektörleri 312

Çizelge 5.54. Karar alternatifleri öncelik sırası 312

Çizelge 5.55. Süreçte rol alan taraflar ve rolleri 313

Çizelge 5.56. Kamu İhale Süreci blokzincir blok yapısı 323

Çizelge **Sayfa**

Çizelge 5.57. Sistem kullanıcıları için üretilen anahtar yapısı örneği 326

Çizelge 5.58. İhale şartları (00) başlıklı ilk (genesis) blok yapısı 327

Çizelge 5.59. İdari şartname (01) başlıklı ikinci blok yapısı 328

Çizelge 5.60. Teknik şartname (02) başlıklı üçüncü bloğun yapısı 328

Çizelge 5.61. Taslak sözleşme (03) başlıklı dördüncü bloğun yapısı 329

Çizelge 5.62. İdareye sorulan sorular (04) başlıklı beşinci bloğun yapısı 330

Çizelge 5.63. İsteklilere verilen cevaplar (05) başlıklı altıncı bloğun yapısı 331

Çizelge 5.64. Geçici Teminat Mektubu (06) başlıklı yedinci bloğun yapısı 332

Çizelge 5.65. Yetki Belgesi (07) başlıklı sekizinci bloğun yapısı 333

Çizelge 5.66. Teklif Mektubu (08) başlıklı dokuzuncu bloğun yapısı 334

Çizelge 5.67. Teklifler-İdari (09) başlıklı onuncu bloğun yapısı 334

Çizelge 5.68. Teklifler-Teknik (10) başlıklı onbirinci bloğun yapısı 335

Çizelge 5.69. Teklifler-Taslak Sözleşme (11) başlıklı onikinci bloğun yapısı 336

Çizelge 5.70. Yüklenici adaylarına sorulan sorular (12) başlıklı onüçüncü bloğun yapısı 337

Çizelge 5.71. İdareye verilen cevaplar (13) başlıklı ondördüncü bloğun yapısı 337

Çizelge 5.72. Teklif Değerlendirme Sonuç Raporu (14) başlıklı onbeşinci bloğun yapısı 339

Çizelge 5.73. Yüklenici Seçim Kararı (15) başlıklı onbeşinci bloğun yapısı 339

Çizelge 5.74. Hyperledger Fabric ve Corda platformlarının temel özellikleri 344

Çizelge 1.1. Süreçte rol alan kurum/birimler ve rolleri 378

Çizelge 1.2. Süreç işlem hacmi 378

Çizelge 1.3. Süreç tarafından üretilen/depolanan veri miktarı 378

Çizelge 1.4. Süreç işlem hızı 379

Çizelge 1.5. Blokzincir üçlü açmazına göre niteliklerin önem dereceleri 379

Çizelge 1.6. Süreç veri içeriği 380

Çizelge 1.7. Süreç verilerinin sınıflandırılması 380

Çizelge **Sayfa**

Çizelge 1.8. Fonksiyonel gereksinimler 381

Çizelge 1.9. Fonksiyonel olmayan gereksinimler 382

Çizelge 1.10. Mevcut süreç/faaliyetle ilgili problemler ya da iyileştirilebilir noktalar .. 382

Çizelge 2.1. Süreçte rol alan kurum/birimler ve rolleri (Kamu İhale Süreci) 383

Çizelge 2.2. Süreç işlem hacmi (Kamu İhale Süreci) 384

Çizelge 2.3. Süreç tarafından üretilen/depolanan veri miktarı (Kamu İhale Süreci) 385

Çizelge 2.4. Süreç işlem hızı (Kamu İhale Süreci) 385

Çizelge 2.5. Blokzincir üçlü açmazına göre niteliklerin önem dereceleri (Kamu İhale Süreci) 386

Çizelge 2.6. Süreç veri içeriği ve veri sınıfı (Kamu İhale Süreci) 386

Çizelge 2.7. Kamu İhale Sürecinde kullanılan veri ve bilgilerin gizlilik dereceleri 388

Çizelge 2.8. Fonksiyonel gereksinimler (Kamu İhale Süreci) 389

Çizelge 2.9. Fonksiyonel olmayan gereksinimler (Kamu İhale Süreci) 390

Çizelge 2.10. Fonksiyonel olmayan gereksinimler (Kamu İhale Süreci) 391

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil 2.1. Merkle ağaç yapısı (ABD Patent No. US4309569A, 1982) 12

Şekil 2.2. 16 işlem için Merkle ağaç yapısı 13

Şekil 2.3. Bitcoin sisteminde blok yapısı 26

Şekil 2.4. Bitcoin'de blok oluşturma işlem adımları 30

Şekil 2.5. Nakamoto (2008) tarafından tarif edilen Bitcoin sistemi ve özellikleri 31

Şekil 2.6. Bitcoin yönetişim modelin basit gösterimi (Perley (2017) "A very rough and simplistic diagram of Bitcoin's governance model"den uyarlanmıştır) 32

Şekil 2.7. İletişim ve mutabakat tercihine göre blokzincir ağları (Usta ve Doğantekin, 2017: 49) 71

Şekil 2.8. Blokzincir çeşitlerinin merkezilik derecesi 72

Şekil 2.9. Blokzincirin uygun çözüm olup olmadığına karar vermek için kullanılan akış şeması (Wüst ve Gervais, 2018). 170

Şekil 2.10. Birch, Brown ve Parulava blokzincir seçim modeli. 170

Şekil 2.11. Hangi tip veri tabanının uygun olduğunu belirlemek için bir model (Koens ve Poll, 2018). 171

Şekil 2.12. Blokzincir kullanımı için karar modeli, Suichies (2015). 172

Şekil 2.13. Blokzincir çözümünün uygunluğu için karar ağacı (Anwar, 2018). 173

Şekil 2.14. Blokzincir çözümü uygunluğu için karar modeli (Mulligan, 2018) 177

Şekil 2.15. AHP işlem adımları (Ho, 2008) 183

Şekil 2.16. AHP hiyerarşik yapısına ilişkin "enerji santrali kararı" örneği (Hämäläinen ve Seppäläinen, 1986) 184

Şekil 2.17. AHP işlem adımları 186

Şekil 2.18. Blokzincir platform seçimi için hiyerarşi modeli (AHP uygulama örneği) . 190

Şekil 3.1. Çalışmanın yöntemi ve kullanılan araştırma teknikleri 218

Şekil 4.1. Model işlem adımları 226

Şekil 4.2. Kullanım senaryosuna göre blokzincir kullanımı için karar akış şeması 232

Şekil 4.3. AHP için örnek hiyerarşik yapı 250

Şekil **Sayfa**

Şekil 4.4. Adım 4. Hesaplama Motoru adımında gerçekleştirilen işlemler 257

Şekil 5.1. Kamu İhale Süreci için blokzincir kullanımı karar ağacı 275

Şekil 5.2. AHP hiyerarşik yapı (ihale süreci, blokzincir çözümü)..... 278

Şekil 5.3. Kamu İhale Süreci blokzincir uygulaması örnek blok yapısı 325

Şekil 2.1. Kamu İhale Sürecinin işleyişi 387

KISALTMALAR

Bu çalışmada kullanılmış kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklamalar
AHP	Analitik Hiyerarşi Prosesi
AML	Anti-Money Laundering - Kara Paranın Aklanmasının Önlenmesi
AMLD5	Anti-Money Laundering Directive - Kara Para Aklamayı Önleme Yönergesi
CBDC	Merkez Bankası Destekli Dijital Paralar
CEN	Avrupa Standardizasyon Komitesi
CENELEC	Avrupa Elektroteknik Standardizasyon Komitesi
CIA	Gizlilik (Confidentiality), Bütünlük (Integrity) ve Kullanılabilirlik (Availability)
DAO	Decentralized Autonomous Organization-Merkezi Olmayan Otonom Kuruluş
DeFi	Decentralized Finance - Merkeziyetsiz Finans
DLT	Dağıtık Defter Teknolojileri
DSA	Digital Signature Standard
EGDI	E-Government Development Index - E-Devlet Gelişmişlik İndeksi
ELECTRE	Elimination et Choix Traduisant La Realite Metodu
EVM	Ethereum Virtual Machine - Ethereum Sanal Makine
GDPR	AB Genel Veri Koruma Yasası
ICO	Initial Coin Offering - İlk Dijital Para Arzı
IEEE	Elektrik ve Elektronik Mühendisleri Enstitüsü
ISACA	Information Systems Audit and Control Association
ITU	Uluslararası Telekomünikasyon Birliği
ITU-T	Uluslararası Telekomünikasyon Birl. Telekomünikasyon Standardizasyon Sektörü
KAYSİS	Elektronik Kamu Bilgi Yönetim Sistemi
KYC	Know Your Customer - Müşterini Tanı
MASAK	Mali Suçları Araştırma Kurulu

Kısaltmalar	Açıklamalar
NFT	Non-Fungible Token - Takas Edilemez Token
NIST	Birleşik Devletler Ulusal Standartlar ve Teknoloji Enstitüsü
PBFT	Pratik Bizanslı Hata Toleransı
PoA	Proof of Authority - Yetki İspatı
PoAs	Proof of Assignment - Atama Kanıtı
PoB	Proof of Burn - Yakma Kanıtı
PoC	Proof of Capacity - Kapasite Kanıtı
PoET	Proof of Elapsed Time - Geçen Zamanın İspatı
PoI	Proof of Importance - Önem Kanıtı
PoS	Proof of Stake - Hisse İspatı
PoW	Proof of Work - İş İspatı
PPP	Public Private Partnership - Kamu Özel İşbirlikleri
RPOW	Reusable Proof-of-Work - Yeniden KullanılabilirİŞ İspatı
SHA	Secure Hash Algorithm
UTXO	Unspent Transaction Outputs - harcanmamış işlem çıktıları

1. GİRİŞ

Blokzincir, ilk ortaya çıktığı 2008 yılından bu yana uygulama sahası sürekli genişleyen, henüz standartları net biçimde ortaya konulmamış ve yasal düzenlemeleri ihtiyacı karşılayacak düzeyde tamamlanmamış olmasına karşın tüm dünyada hem kamu hem de özel sektör tarafından yakından takip edilen bir teknolojidir. Yakın gelecekte birçok sektörü etkilemesi, günümüzdeki birçok iş alanının ortadan kalkmasına ya da dönüşmesine sebep olması öngörülmekte olup bu nedenle de yıkıcı bir teknoloji olarak adlandırılmaktadır.

Kamu hizmetlerinin elektronik ortamda sunulması olarak tanımlanan e-devletin yerini artık işlemleri kolaylaştırmak ve etkinliğini artırmak için kurumlar arasındaki hizmetlerin entegre edilmesi, birden fazla kurum ya da kuruluşun sorumlu ya da paydaş olduğu işlemlerin birbirine entegre bir biçimde, daha kolay erişilebilir ve hızlı olarak sunulması olarak özetlenebilecek dijital devlet kavramı almaktadır. Verimliliği artırmak, maliyetleri düşürmek ve rekabet gücünü artırmak amacıyla faaliyet gösterme ve vatandaşlara değer sunma şeklini temelden değiştirmek için teknolojiyi kullanma süreci ise dijital dönüşüm olarak adlandırılmaktadır.

Dijital dönüşüm, bulut bilişim, büyük veri analitiği, yapay zekâ, blokzincir ve nesnelerin interneti dâhil birçok teknolojiyi kapsayabilir. Ayrıca organizasyon yapılarında, iş modellerinde ve süreçlerde değişiklikler içerebilir. Dijital dönüşümün nihai hedefi, dijital teknolojinin yeteneklerinden yararlanarak büyüme ve yenilik için yeni fırsatlar yaratmaktır. Blokzincir teknolojisi, bu dönüşümün bir parçası olarak kullanılabilecek özel bir dijital araçtır. Blokzincir, tedarik zinciri, finans, sağlık hizmetleri, kimlik yönetimi ve daha pek çok farklı sektörde kullanılabilirdir. Kısacası blokzincir, güvenli ve verimli dijital işlemler için gerekli altyapıyı verileri depolamak ve paylaşmak, işlemleri kolaylaştırmak ve süreçleri otomatikleştirmek için güvenli ve şeffaf bir yolla sağlayarak dijital dönüşümde rol alan bir teknolojidir.

En önemli avantajları arasında sayılan işlemlerin şeffaflığı, işlem kayıtlarının silinmesinin ya da değiştirilmesinin mümkün olmaması, işlemlerin merkezi bir otorite ya da üçüncü bir taraf kontrolünden ya da onayından bağımsız bir biçimde gerçekleştirilebilmesi, blokzincirin birden fazla taraf arasında gerçekleştirilen iş süreçlerinde kullanımını cazip hale

getirmektedir. Bunla birlikte, teknolojinin karmaşıklığı, tek bir tasarım ya da konfigürasyona sahip olmaması nedeniyle anlaşılmasının ve uygulanmasının güçlüğü, henüz standartlarının ve finans gibi bazı kullanım alanlarında yeterli mevzuat düzenlemesinin bulunmaması, hacimli veri içeren ve çok hızlı biçimde gerçekleştirilmesi istenen süreçler için uygun olmaması, kaydedilen verilerin hatalı bile olsa değiştirilememesi ve silinememesi gibi etkenler ise kullanımının önündeki engelleri oluşturmaktadır.

Blokzincir teknolojisinin seçilen bir süreç için uygulanması kararı verilirken bu avantajlar ve kısıtlar dikkate alınmalı, herhangi bir yatırım gerçekleştirilmeden önce, kaynakların en etkin biçimde kullanılabilmesi için tüm olumlu ve olumsuz yönler ile fırsatlar ve tehditler sistematik bir biçimde değerlendirilmelidir. Gerekli ön değerlendirme yapılıp sürecin blokzincir ile tasarıma uygun olup olmadığı analiz edilmeden, yeterli ön çalışma ve ön hazırlık yapılmadan blokzincir ile uygulama geliştirilme kararı verilmesi mali kaynakların ve zamanın etkin biçimde kullanılamaması riskini taşımaktadır. Bu nedenle, bu teknolojinin uygulanması kararı verilirken sürecin blokzincire uygun olup olmadığı, uygun olması halinde hangi platformun en uygun tercih olacağı gibi unsurları içeren kararı destekleyici çıktıyı sunan bir model geliştirilmesine karar verilmiştir.

Blokzincirin her sürece uyan tek bir çözüm olmadığı ve dijital dönüşümü yönlendirmek için kullanılabilecek çeşitli araçlardan biri olarak düşünülmesi gerektiği unutulmamalıdır. Kurumlar, blokzincirin özel ihtiyaçlarını karşılamak için doğru teknoloji olup olmadığını ve faydalarının maliyetlerinden ve zorluklarından ağır basıp basmadığını değerlendirmelidir.

Bu çalışmanın amacı, seçilen herhangi bir kamu hizmeti süreci için blokzincir teknolojisinin kullanımının uygun olup olmadığını tespit eden, uygunluk halinde platform alternatiflerini kullanıcı önceliklerine göre sıralayan ve en uygun alternatife ilişkin blokzincir tasarımını ortaya koyan bir model önerisi sunmaktır.

Bu tez çalışmasında, sunduğu avantajlar kadar kısıtlılıkları da dikkate alınarak blokzincirin uygulanabilir olup olmadığı konusunda objektif değerlendirme yapılmasına yardımcı olan, değişken kullanıcı tercihleri ve çözüm alternatiflerine uyarlanabilir ve teknik detayları konusunda derin bilgi sahibi olunmadan da kullanılabilir bir model geliştirilmesi hedeflenmiştir.

Blokzincir teknolojisi ile bir uygulama geliştirilirken detaylarına İkinci Bölümde yer verilmiş olan bazı teknik konular ve hedeflenen sonuçlara ulaşmak için en uygun mimari özellikler dikkate alınmalıdır. Teknolojinin kullanımına karar verilmesi ve bu kararı takiben sistemin tasarlanması aşamalarında, henüz gerekli kaynaklar tahsis edilip planlama aşamasına geçilmeden önce çözülmesi gereken bazı problemler ve verilmesi gereken kararlar bulunmaktadır. İlk aşamada cevap verilmesi gereken sorular özetle aşağıdaki biçimdedir:

- Blokzincir teknolojisinin tüm fayda ve dezavantajları, en uygun kullanım alanları, teknik özellikleri ve farklı platformların özellikleri teknolojinin kullanım kararını vermeyi destekleyici düzeyde biliniyor mu?
- Mevcut süreç ya da faaliyetle ilgili problemler ya da iyileştirilebilir alanlar nelerdir? Bu problemlerin çözümünde ya da ilgili sürecin iyileştirilmesinde blokzincirden faydalanılabilir mi?
- Blokzincir teknolojisinin uygulanması için kullanılabilecek alternatif çözümler nelerdir? Bu alternatiflerin değerlendirilebilmesi için hangi özellikleri dikkate alınabilir?
- Blokzincir teknolojisinin uygulanmasında süreç sahibi için hangi kriterler, ne derecede önemlidir? Bu kriterlerin önem derecelerini dikkate alarak en uygun çözüm alternatifini seçmek için hangi yöntemlerden, nasıl faydalanılabilir?
- Seçilen kriterler ve bu kriterleri karşılayan alternatifleri bir arada değerlendirerek en uygun çözümü önermek için hangi yaklaşımlardan faydalanılabilir?
- En uygun çözüme ilişkin tasarım nasıl olmalıdır?

Önerilen model ile yukarıda sıralanmış olan soruların yanıtları girdi, işlem ve çıktı döngüleri biçiminde sunulmaktadır.

Herhangi bir uygulama için kullanılacak en uygun blokzincir platformunun seçimi, mevcutta çok sayıda platform bulunması ve bu sayının sürekli olarak artması nedeniyle önemli bir problemdir. Bu seçim güçlüğü problemlerine sistematik bir çözüm getirmek amacıyla blokzincir platformları ile ilgili bilgilerin toplanması ve toplanan bilgilere göre birbirleri ile karşılaştırılmaları için sistematik bir yaklaşım önerilmektedir.

Karara etki eden seçim kriterleri ve bunların önem dereceleri ile çözüm alternatifleri verilecek kararın hızı ve uygunluğuna etki eden temel faktörlerdir. Öte yandan, bu kriterlerin

ve alternatiflerin belirlenmesi ve bunlar hakkında bilgi toplanması zaman alıcı bir süreçtir. Seçim kriterlerinin önem derecelerinin belirlenmesinde karar vericilerin sübjektifliği, çözüm alternatiflerine ilişkin toplanan bilgilerin doğruluğu ve güvenilirliği karar verme sürecinin çıktısını doğrudan etkileyen unsurlardır. Karar verici sübjektifliğini en aza indirmek için kriterlerin önem derecelerinin belirlenmesinde grup kararı, uzman desteği ya da oylama, alternatiflerin özelliklerinin güvenilirliği ve doğruluğu için de uygun araştırma yöntemleri ile bilgi toplama ve kaynaklar arasında karşılaştırmalı analiz önerilmektedir. Çözüm alternatiflerine ilişkin bilgilere yönelik bir diğer kısıt, blokzincir teknolojisinin nispeten yeni olması, platform alternatiflerinin bir kısmının henüz kendini kanıtlamış bir uygulaması bulunmaması, bu platformlara ilişkin yeterli veri ve bilginin bulunmamasıdır. Bu nedenle, bu çalışma için alternatiflerin belirlenmesinde yeterli ve güvenilir bilgi kaynağına erişilebilirlik ön koşul olarak değerlendirilmiş, platform alternatiflerinin seçimi bu koşula dayalı olarak yapılmıştır.

Karar verme sürecinin karmaşıklığına, dolayısı ile sonucuna etki eden bir diğer faktör ise kriter sayısının ve alternatif adedinin artmasıdır. Kriter ve alternatif sayısının fazlalığı kararın hassasiyeti ve güvenilirliğine olumlu etki etmekle birlikte, karar verme sürecinin daha karmaşıklaşması ve daha uzun zaman alması gibi handikapları da bulunmaktadır. Bu nedenle, önerilen modelde öncelikle karar kriterlerine göre alternatifler arasında bir ön eleme yapılmakta, belirli şartları istenen ölçüde sağlamayan adaylar alternatifler arasından çıkarılarak işlemlerin karmaşıklığı azaltılmaktadır.

İncelenmiş olan literatür, küresel öncü firmaların yapmış oldukları çalışmalar ve hazırladıkları raporlar, Avrupa Birliği ve Birleşmiş Milletler tarafından yürütülen çalışmalar, bilgi teknolojileri ve bilgi güvenliği gibi konularda faaliyetler yürüten uluslararası kuruluşların çalışma ve raporları blokzincirin sürekli artan bir ilgi ile üzerinde yoğun biçimde çalışılan bir teknoloji olduğunu göstermektedir. Bu teknolojiden faydalanacak olan taraflar ile teknolojinin hâlihazırda yürüttükleri faaliyetleri ve gelir kaynaklarını tehdit ettiği bankacılık gibi sektörler hem uygulama geliştirerek sistemin avantajlarından faydalanmak hem de sistemin getireceği riskleri en aza indirmek için yoğun uğraş vermektedirler. Özellikle kamu sektörü uygulamaları konusunda henüz başlangıç aşamasında olan bu teknolojinin daha iyi anlaşılması gerekliliği, kullanımı konusunda akademik olarak ülkemizde yapılmış olan çalışmaların daha çok dijital para ile sınırlı olması ve konuyu derinlemesine inceleyerek dünyadaki gelişmeleri içine alacak biçimde bilgilendirici ve

yönlendirici bir çalışma bulunmaması bu tez çalışmasının konusunun seçiminde önemli bir etken olmuştur.

Yeni teknolojilerin mevcut süreçlerde uygulanması konusunda karar vericiler için en genel ve temel iki risk bulunmaktadır: fırsatların kaçırılması güdüsü ile teknolojinin uygulanmasında aceleci davranılarak kaynakların uygun olmayan biçimde harcanması, temkinli davranarak bekle ve gör stratejisi izlenmesi sonucunda teknolojinin sunduğu fırsatların kaçırılması. Önerilen modelin kamu sektörü uygulamaları ve karar vericileri için her iki riskin de etkisinin ve olasılığının uygun biçimde değerlendirilmesi ve en uygun kararın verilerek bu risklerin etkileri ve olasılığının düşürülmesine katkıda bulunması hedeflenmektedir. Herhangi bir kamu uygulaması için yatırım kararı verilmeden önce önerilen modelin kullanılarak çıktıların değerlendirilmesinin kamu kaynaklarının etkin biçimde kullanımına katkı sağlaması beklenmektedir.

Seçilen bir kamu hizmeti süreci için blokzincirin kullanılabilir olup olmadığı, kullanılabilir olması halinde kullanıcı öncelikleri dikkate alınarak hangi blokzincir platformunun en uygun çözüm olduğu sonucunu vererek ve çözümün temel mimarisinin sunulması hedeflenerek önerilen model beş temel adımdan oluşmaktadır. Modelin ilk aşamasında, sonraki adımlarda kullanılmak ve seçim kurallarına temel oluşturmak üzere blokzincirin kullanım alanları, avantajları, kısıtlılıkları, blokzincir uygulamalarında kullanılan önemli platformların özellikleri derlenmektedir. İlk adımda listeler biçiminde hazırlanan bu özellikler daha sonra değişiklik yapmaya, güncellemeye ve genişletmeye uygun yapıdadır. Modelin ikinci adımında ilk adımda belirlenen özellikler doğrultusunda seçim kuralları geliştirilmiştir. Bu kurallar blokzincirin uygun çözüm olup olmadığı kararı için kullanılan temel seçim listelerini ve bir karar ağacını, platform özelliklerini içeren karşılaştırma tablosunu ve Çok Kriterli Karar Verme metotlarından biri olan Analitik Hiyerarşi Prosesinin işlem adımlarını içermektedir. Modelin üçüncü adımında süreç seçimi yapılarak hesaplamalar için gerekli olan kullanıcı girişlerini içeren dış bilgi bir form aracılığı ile alınmakta, sürecin mevcut özellikleri, beklenen özellikler ve kullanıcı tercihleri ile seçim kriterlerinin öncelik değerleri için veriler toplanmaktadır. Dördüncü adımda, üçüncü adımda toplanan veriler ikinci adımdaki kurallar doğrultusunda değerlendirilerek seçim kriterlerinin önceliklerine göre platform alternatifleri birbirleri ile karşılaştırılmakta, bu karşılaştırma sonuçları sayısal sonuçlarla ifade edilerek çözüm alternatifleri sıralanmaktadır. Son adımda ise önceki

adımlarda elde edilen sonuçlar bir araya getirilerek kullanıcı tercihlerine uygun blokzincir mimarisi ortaya konmaktadır.

Tezin İkinci Bölümünde "Kavramsal Çerçeve ve İlgili Araştırmalar" başlığı altında blokzincir teknolojisinin detayları, standardizasyon ve yasal düzenleme çalışmaları, uluslararası kuruluşlar ve devletlerce yürütülen çalışmalar, Türkiye'de blokzincir çalışmaları, kamu hizmetlerinde kullanım potansiyeli, blokzincirin kullanılabilirliğine yönelik karar modelleri ve Çok Kriterli Karar Verme metotlarından bahsedilmektedir. Üçüncü Bölümde yöntem açıklanmakta, Dördüncü Bölümde ise blokzincir teknolojisinin kullanımı için önerilen modelin işlem adımları verilmektedir. Beşinci Bölümde, önerilen modele göre seçilen bir kamu hizmeti için blokzincirin kullanılabilirliği değerlendirilmekte, model işlem adımları uygulamalı olarak gösterilmektedir. Tez, Sonuç ve Öneriler kısmı ile sona ermektedir.

2. BLOKZİNCİR TEKNOLOJİSİNİN ÖZELLİKLERİ VE ÇOK KRİTERLİ KARAR VERME

2.1. Blokzincir Teknolojisi

Çarkacıoğlu (2016: 42, 45) blokzinciri herkese açık, şeffaf, dağıtık, sıralı ve zaman damgalı Bitcoin transfer işlemlerini içeren dijital küresel hesap defteri, düz bir veri dosyası, basit bir veritabanı olarak tanımlamaktadır. Bitcoin'le beraber ortaya çıkan, farklı kullanım alanları da olan blokzincir teknolojisi merkezi olmayan bir ağ yapısındaki uç bilgisayarlarda, birbirinden bağımsız olarak saklandığından, herhangi bir merkezi hatadan kaynaklanacak problemlere karşı dirençlidir.

Ethereum'un kurucusu Vitalik Buterin'in belirttiği biçimde, çoğu teknoloji basit görevleri yerine getiren çalışanların işlerini otomatikleştirme eğilimindeyken blokzincir ise merkezi otomatikleştirmektedir. Taksi şoförlerini işten çıkarmak yerine, blokzincir Uber'in işine son vererek taksi şoförlerinin doğrudan müşteri ile çalışmasına izin vermektedir (Kirshbaum, 2016).

Blokzincir işlem kayıtlarını kronolojik olarak blokzincir ağındaki tüm makineler üzerinde özdeş olarak kaydeden, verilerin bir defa kaydedildikten sonra değiştirilmesine ve silinmesine izin vermeyen, işlemlerin doğrulanması ve onaylanmasının ağdaki makineler tarafından gerçekleştirildiği bir kayıt sistemidir.

Blokzincir teknolojisinde işlem gerçekleştirilirken öncelikle işlemler ya da veriler gruplanarak metadata verisi ve önceki bloğun parmak izi ile birlikte blok biçimde toplanır, işlem zamanlarına göre zaman damgası ile işaretlenir ve işlemlerin doğruluğunun onaylanması için ağda yayınlanır. Her bir blok kendisinden önceki bloğun hash değerini içerdiğinden bir bloktaki en küçük bir değişiklik kendisinden sonraki tüm blokların yapısını değiştirir. Daha önceki bloklardaki herhangi bir veriyi değiştirmek, takip eden tüm bloklardaki verileri değiştirmeyi ve bu değişikliği ağdaki tüm kullanıcılarda kaydedilen kopyalarda yinelemeyi gerektirir. Bu da pratikte çok zor bir işlemdir. Tamamlanan her blok ile birlikte en güncel zincir ağdaki katılımcılar tarafından kopyalanır. Herhangi bir katılımcıda hatalı, manipüle edilmiş ya da bozulmuş bir veri zincirinin bulunması sistemi

tehlikeye atmaz. Bilgilerin gizliliği ve bütünlüğü kriptoloji ile sağlanır (Karahan ve Tüfekci, 2019).

Iansiti ve Lakhani (2017) blokzincir teknolojisinin dayandığı beş prensibi dağıtık veri tabanı, eşten eşe iletim, takma adla şeffaflık, kayıtların geri döndürülmezliği, hesaplamaya dayalı mantık olarak sıralamaktadır. Blokzincir teknolojisinde, ağ içerisindeki her katılımcı veri tabanının tümüne ve tüm geçmiş verilerine erişim sağlayabilir. Veri ya da bilginin kontrolü tek bir tarafta değildir. Herhangi bir aracıya gerek olmadan kayıtların ya da işlemlerin doğruluğu teyit edilebilir. İletişim doğrudan eşler arasındadır. Blokzincirde her kullanıcı ya da düğümün 30'dan fazla sayıda alfanümerik karaktere sahip benzersiz bir adresi vardır. Blokzincirde işlemler bu adresler vasıtasıyla gerçekleştirilir. Kullancılar anonim kalmayı ya da kendi istedikleri taraflar ile kimliklerini paylaşmayı seçebilirler. Bir işlem veri tabanına bir defa girdikten ve kayıtlar güncellendikten sonra, her bir kayıt bloğu birbirlerine bağlı olduğundan kayıtlar değiştirilemez. Blokzincir işlemlerinin gerçekleştirilmesi otomatik olarak çalışan algoritmalar ve kuralları kullanan hesaplama mantığına dayalıdır.

Ribeiro ve Nakamura (2019) blokzincir teknolojisinin üzerine inşa edildiği dört ana mimari özelliği işlemlerin gizliliği, merkezsizleşmiş depolama ve hesaplama işlemleri, veri bütünlüğü ve işlemlerin değiştirilemez ve silinemez oluşu olarak sıralayarak blokzinciri eşler arası bir ağdaki bilgisayarlarda eş kopyaları tutulan gerçeklerin kayıt defteri olarak nitelendirmekte, özelliklerini aşağıdaki biçimde sıralamaktadır:

- Kayıt defteri, bir defa onaylandıktan sonra asla silinemeyecek kayıtları içeren dijital bir defterdir.
- Deftere kaydedilen gerçekler parasal bir işlem, belirli bir belge içeriği, bir bilgisayar kodu ve hatta bazı platformlarda küçük bir veri tabanı bile olabilir.
- Ağdaki katılımcılar anonim olabilirler ve bunlara eş ya da düğüm adı verilir.
- Kayıt defterindeki her işlem işlemin göndericisi ve alıcısı bilgilerini de içeren kriptografik bir dijital imza ile korunur.
- Herhangi bir düğüm, kayıt defterine bir gerçek eklemek istediğinde bu gerçeğin deftere eklenip eklenmeyeceğine karar vermek için düğümlerin tamamı ya da belirli bir kısmının mutabakatına gerek duyulur.
- Mutabakat sağlanırsa, gerçek bir daha silinmeyecek biçimde kayıt defterine yazılır.

Blokzincir teknolojisinden bahsedilirken genellikle merkezsizleşmiş (decentralized) ve dağıtık (distributed) terimleri birbirine karıştırılmaktadır. Merkezsizleşmiş sistemlerde her düğüm kendi kararını verir. Bu sistemlerde ağ varlıkları üzerindeki kontrol birden çok düğüm arasında dağıtılarak yüksek hata toleransı sağlanır. Blokzincirde merkezsizleşmiş kontrolün temeli blokların ağdaki düğümler arasında adil bir biçimde oluşturulması, doğrulanması ve doğrulama hakkının dağıtılmasından oluşur. Sistemin nihai davranışı bireysel düğümlerin kararlarının toplamıdır. Sistemde merkezi bir kontrol bulunmamaktadır. Merkezsizleşmiş sistemlere örnek olarak Bitcoin ve Tor ağı verilebilir. Merkezsizleşmiş sistemlerde kolektif görevleri yürütmek güçtür. Küçük sistemler için çok uygun olmayan bu sistemler yüksek erişilebilirliğe sahiptir. Merkezsizleşmiş sistem dağıtık sistemin bir alt kümesidir. İkisi arasındaki temel fark kararların nasıl verildiği ve sistemdeki düğümlerde bilginin nasıl paylaşıldığıyla ilgilidir. Dağıtık sistemlerde veri depolama, hesaplama gibi işlemler çok sayıda düğüm arasında paylaşılmıştır ancak merkezi bir süreç sistemi yönetir ve kararlar merkezi bir biçimde verilebilir.

Merkezsizlik blokzincir teknolojisinin temel özelliklerinden biridir. Bitcoin örneğinde olduğu gibi blokzincir ağı internet üzerinde eşler arası (P2P) ağ olarak yapılandırılmıştır. Eşler arası ağ, ağa katılan her bilgisayarın eşit olduğu ve hepsinin ağ hizmeti sağladığı anlamına gelmektedir. Burada, ağ topolojisi eşlerin birbirlerine bir ağ örgüsü biçiminde, merkezi bir hizmet ya da hiyerarşi olmadan bağlandığı, ağa katılımın karşılıklı olarak teşvik edildiği düz bir ağdır. Eşten eşe ağlar doğası gereği dirençli, merkezsizleşmiş ve açıktır. Blokzincir ağındaki düğümler birbirine eşit olmakla birlikte destekledikleri fonksiyona bağlı olarak farklı roller üstlenebilirler. Düğümlerin üstlenebilecekleri bu farklı roller aşağıdaki biçimdedir:

- Yönlendirme: Ağdaki her düğüm işlemlerin doğrulanması, ağda yayılması, eşlerle bağlantı sağlanması için mesajları alıp ileten bir yönlendirici fonksiyonuna sahiptir.
- Blokzincir veri tabanının tutulması: Bazı düğümler blokzincirdeki paylaşılan kayıt defterinin bir kopyasını tutarak bağımsız ve yetkili bir biçimde işlemleri doğrularlar.
- Madencilik: Düğümlerden bir kısmı yeni bloklar oluşturulması sürecine katılarak madenci olarak hizmet ederler.
- Uygulamaya özel fonksiyonlar: Ağdaki bazı düğümler dijital cüzdan ya da akıllı sözleşme gibi uygulamaya özel fonksiyonları çalıştırırlar. Madenci düğümlerle benzer

biçimde bu düğümler blokzincirin bir kopyasını tutarak madencilik sürecine de katılabilirler.

Blokzincir teknolojisi temelinde, her yeni işlemin, bir başka işlemin çıktısını girdi olarak almaya zorlayan bir çeşit veri tabanıdır. Bitcoin'de bu kural harcanmamış işlem çıktıları (Unspent Transaction Outputs - UTXO) modeli ile uygulanır. Bu özellik sayesinde işlemler başlangıç bloğuna kadar izlenebilirdir ve özellikle şeffaflık, denetlenebilirlik ve izlenebilirliğin önemli olduğu alanlarda çok faydalıdır. Yeni bir blok yaratıldığında bu blok kendinden önceki bloğun referansını içerir. Bu nedenle blokzincirde depolanan veri kronolojik bir sırada ve sadece veri eklemeye izin veren bir yapıdadır. Blokzincir teknolojisi veri yapısının bir diğer özelliği en uzun zincir kuralıdır. Belirli bir bloktan başlangıç bloğuna kadar gitmek için tek bir yol bulunur.

Blokzincir teknolojisi her biri "hash" adı verilen kriptografik parmak izini içeren işlemlerin benzersiz bir kümesini içeren bir bloklar zinciridir. Her bir blok geçerliliği onaylanmış işlemleri içermekte olup içindeki bilgiler erişilebilir ancak değiştirilemezdir.

Bloklar zincire otomatik olarak eklenmezler. Yeni bloklar "madencilik" adı verilen bir prosesle yayınlanırlar ve bu süreç madenci düğümler tarafından yürütülür. Bir düğüm tarafından bir işlem başlatıldığında bu diğer düğümler tarafından gözden geçirilerek onaylanır. Daha sonra, bu işlem diğer bekleyen işlemlerle birlikte daha önceki işlem grubu doğrulanarak bir bloğa ekleninceye kadar kuyrukta bekletilir. Daha sonra madenci düğüm doğrulanmış bloğu ağda yayınlar. Bloğun yayınlanmasından sonra madenci düğüm bloğu ağın geri kalanına yayınlamaya başlar. Madenci düğümler geçersiz işlemleri kabul etmez ve bunları bloğa eklemez, dolayısı ile bu işlemler ağda yayınlanmazlar. Bu süreç karmaşık görünmekle birlikte genellikle blokzincir yazılımı tarafından otomatik olarak yapılır. Madencilik prosesinin sıklığı ve diğer bazı parametreleri (blokta kaç işlemin yer aldığı ve kuyrukta ne kadar süre bekledikleri gibi) blokzincir platformunun nasıl tasarlandığına bağlı olarak farklılık gösterir.

2.1.1. Blokzincir teknolojisinin tarihçesi

Blokzincir teknolojisinin tarihçesinden bahsedilirken genellikle Bitcoin ile başlanmakla birlikte, blokzincire uzanan yolun başlangıcı çok daha eskilere gitmektedir. Oyun teorisi,

olasılık teorisi, kriptografi ve eşten eşe ağlar blokzincir teknolojisinin temelini oluşturması nedeni ile dolaylı olarak, takip edilmesi mümkün olmayan ödemeler, dijital para geliştirme, merkezi olmayan bir para sistemi geliştirme, zaman damgası ile dijital dokümanların bir zincir biçiminde sıralanması gibi konularda yapılan çalışmalar ise doğrudan bu tarihçenin içerisinde yer almaktadır.

Kripto para birimlerinin gelişiminin temel taşlarından biri olan oyun teorisi aynı zamanda Bitcoin sisteminin ortaya çıktığı 2009 yılından günümüze dek ayakta kalmasının en önemli nedenlerinden biridir. Oyun teorisi, insan davranışını rasyonel karar verme temelinde incelemek, potansiyel davranış ve kararların olası sonuçlarını araştırarak en makul çözümü bulmak için kullanılan uygulamalı bir matematiksel yöntemdir. Başta kripto paralar olmak üzere blokzincir uygulamalarında oyun teorisi güvenilir bir aracıya ihtiyaç duymadan güvenin inşa edilmesinde önemli bir rol oynar. Oyun teorisinin temelinde yatan toplam refahı artırmak için hem bireysel çıkarın hem de ait olunan toplumun çıkarının düşünülerek ona göre hareket edilmesi gereksinimi blokzincirde hem madenciler ve diğer ağ üyeleri gibi ekosistemin içerisindeki unsurların ilişkilerinin düzenlenmesinde, hem de ekosistemin üyesi olmayıp da blokzincir ağına zarar vermek isteyen kötü niyetli saldırganların girişimlerinin önlenmesinde kullanılmaktadır. Liu ve diğerleri (2019) blokzincir ağındaki yaygın sorunların üstesinden gelmek için oyun teorisinden faydalanıldığını belirterek bu sorunlar arasında bencil madencilik, %51 saldırısı, hizmet reddi (DoS) saldırısı, hesaplama gücü tahsisi, ödül tahsisi, havuz seçimi gibi madencilik faaliyetinin yönetimi, blokzincir ekonomisini saymaktadır.

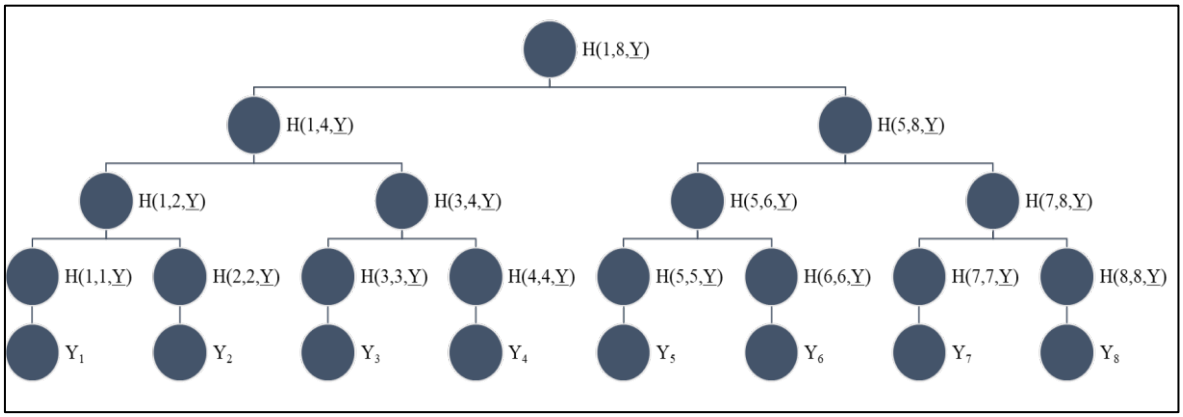
Blokzincir teknolojisinin ilk gerçek hayat uygulaması olan Bitcoin blokzincir mimarisinde zincirin güvenliğinin sağlanması, alternatif bir zincir yaratarak zinciri manipüle etmek isteyen bir saldırganın başarı olasılığının düşürülmesi için olasılık teorisinden faydalanılmaktadır. Bitcoin tasarımında William Feller'in 1957 tarihli "Olasılık Teorisi ve Uygulamalarına Giriş" adlı kitabından faydalanılmış, makalenin referansları arasında bu kitaba da yer verilmiştir.

Blokzincir teknolojisinin ana omurgasını oluşturan unsurlardan biri olan kriptografi ilk olarak Diffie ve Hellman (1976, 1979) tarafından ortaya konulan yeni anahtar değişimi tekniği ile devlet kontrolü dışında kullanılabilir hale gelmiştir. Diffie-Hellman anahtar değişimi olarak bilinen yöntem karşılıklı iki tarafın güvenli olmayan bir iletişim hattı

üzerinden birbirleri ile ortak bir gizli anahtar üretmelerini, bu anahtar kullanılarak güvensiz olan bu hat üzerindeki iletişimin şifrelenmesini sağlamaktadır. Açık anahtarlı sistem güvenli iletişim, şifreleme ve dijital imza gibi günümüzde de kullanılan birçok tekniğin temelinde yatan, kriptolojide çığır açan bir sistemdir.

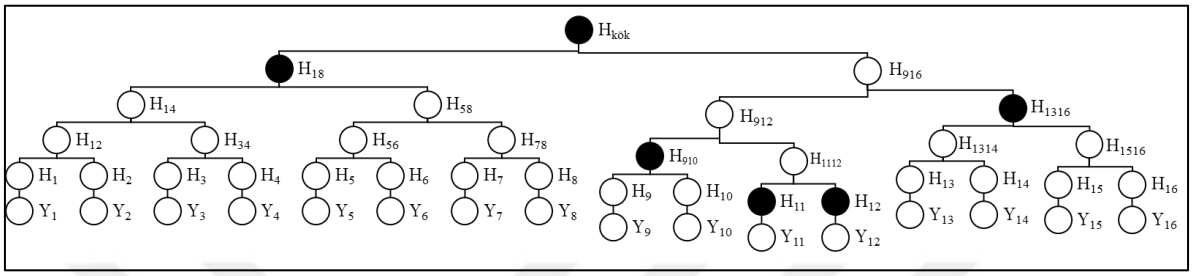
Blokzincir teknolojisinin ana unsurlarından bir diğeri Merkle ağaç yapısı ve Merkle kökü kavramıdır. Temelinde, büyük hacimli verilerin doğrulanması için tek yönlü bir fonksiyon ile ağaç yapısı biçiminde dijital imzanın kullanılmasına dayalı Merkle ağaç yapısı, dağıtık sistemler için doğrulama işlemini çok etkin bir biçimde gerçekleştirmektedir. Bu doğrulamanın etkinliği veri ya da dosyanın tamamı yerine güvenli özet (hash) değerlerinin kullanılmasından kaynaklanmaktadır.

Ralph Merkle tarafından ortaya konulan bu yapı için 1979 yılında patent başvurusu yapılmış, 1982 yılında patent başvurusu onaylanmış, patentin süresi 1999 yılında sona ermiştir. Temel olarak binary ağaç yapısına benzer biçimde çalışan Merkle ağaç yapısında veri bloklarının önce tek tek hash değerleri alınmakta, daha sonra her bir blok ikişerli olarak yeniden hash fonksiyonuna sokulmakta, bu işlem en tepede Merkle kökü adı verilen tek bir hash değeri elde edilinceye dek sürdürülmektedir. Merkle ağaç yapısının basit bir gösterimi Şekil 2.1'de verilmiştir. Gönderilen bu veri bloklarının doğrulanması için ise veri bloklarının tamamının yeniden hash değeri alınarak tek tek karşılaştırma yapılmasına gerek kalmamakta, Merkle kökü ile birlikte sadece "$\log_2$(veri bloğu sayısı)+1" adet veri bloğunun doğrulanması yeterli olmaktadır (ABD Patent No. US4309569A, 1982).



Şekil 2.1. Merkle ağaç yapısı (ABD Patent No. US4309569A, 1982)

Merkle kökü ve ağaç yapısı Bitcoin'de bloğun içerdiği işlemlerin doğrulanmasında kullanılır. Nakamoto (2008) Bitcoin'i ilk defa duyurduğu makalesinde Merkle ağacının sadece kök değerinin bloğun hash değerine dahil edildiğini, işlemlere ait hash değerlerinin depolanmasına gerek olmadığını belitmektedir. Bitcoin'de Merkle ağacının kullanımına ilişkin örnek Şekil 2.2'de verilmiştir.



Şekil 2.2. 16 işlem için Merkle ağaç yapısı

Şekil 2.2'de verilmiş olan örnek Merkle ağaç yapısı Bitcoin sistemindeki bir bloğun içerisinde yer alan 16 işlemi ifade etmektedir. Bu yapıda, blok içindeki tüm işlemlerin doğrulanmasına gerek duyulmamakta, işlemlerin tamamının doğruluğu için $Log_2(16)+1 = 5$ adet hash değerinin kontrol edilmesi yeterli olmaktadır.

Kriptografik hash fonksiyonunun bir veri parçasına art arda uygulanması hash zinciri olarak adlandırılmaktadır. Hash zinciri tek bir anahtar ya da paroladan çok sayıda tek seferlik anahtar üretmek için kullanılan bir yöntemdir. 1981 yılında Leslie Lamport tarafından geliştirilen bu yaklaşım güvensiz bir ağda bilgisayarların güvenli oturum açmaları için bu tek kullanımlık anahtarları kullanmaktadır. Bitcoin Merkle ağaç yapısı ile birlikte bu yaklaşımdan da faydalanmaktadır. Lamport (1981) çalışmasında hash zincirlerinin güvensiz bir ortamda şifre güvenliğinin sağlanması için kullanımını şu biçimde anlatmaktadır: Kimlik doğrulamaya gereksinim duyan bir sunucu, şifrenin iletişim esnasında ya da sunucudan çalınmasını engellemek üzere, düz metin biçiminde tutmak yerine hash zinciri yapısını tutar. Örneğin; sunucu, kullanıcı tarafından sağlanan $hash^{1000}$(şifre) değerini tutmakla başlar. Kullanıcı oturum açmak istediğinde sunucuya $hash^{999}$(şifre) değerini iletir. Sunucu bu durumda hash($hash^{999}$(şifre)) fonksiyonu ile $hash^{1000}$(şifre) değerini hesaplar ve kendinde tuttuğu hash değeri ile karşılaştırarak doğrulamayı gerçekleştirir. İletişim esnasında $hash^{999}$(şifre) değerinin çalınması bir risk doğurmaz çünkü sunucu artık $hash^{998}$(şifre) değerini beklediğinden kimlik doğrulama için aynı hash zinciri sunucuya yeniden iletilemeyecektir. Buterin (2013) bir şifrenin hash değerini yayınlamayı halka açık bir kilit

koymaya, orijinal değerin serbest bırakılmasını da bu kilidin tekrar kapatılamayacak biçimde açılmasına benzetmektedir. Buradaki sorun, kilitlerin kendiliğinden güvenli bir dijital imza oluşturamaması, gereksinim ise orijinal değeri ortaya çıkarmadan matematiksel bir kilidin ardındaki gizli değere sahip olunduğunun kanıtlanması, bu kanıtın da mesaja eklenmesidir. Bu mesaj Bitcoin'deki işleme karşılık gelmektedir. İstemci, Bitcoin'de ağa bir işlem gönderdiğinde aslında yaptığı şey gerçeğin matematiksel bir kanıtını göndermektir. İşte bu çözümü geleneksel herhangi bir açık anahtarlı şifreleme sistemi olmadan sağlayan yapı Lamport imzası olarak da bilinen hash zinciridir.

Hash zincirinin Unix'te oturum açmak için kullanılan biraz daha gelişmiş ve iyileştirilmiş bir versiyonu 1994 yılında Neil Haller tarafından yayınlanan, bir makale ile tanıtılmıştır. Haller (1994) "S/KEY Tek Seferlik Şifre Sistemi" başlıklı makalesinde bu sistemi ağda sadece tek kullanımlık şifrenin geçtiği, oturum açma sırasında ya da kimlik doğrulama gerektiren komutlar kullanılırken kullanıcının gizli parolasının hiçbir zaman ağdan geçmediği, bu nedenle ağ dinleme ve tekrarlama saldırılarına karşı dirençli bir sistem olarak tarif etmektedir. Korunması amaçlanan ana sunucu da dahil olmak üzere hiçbir sistemde gizli bilgilerin depolanmasına gerek bulunmamaktadır.

Bitcoin'in yaratılmasına uzanan yolda çalışmalarından faydalanılan bir diğer isim "Kriptonun Babası" (Godfather of Crypto) olarak da bilinen David Chaum'dur. Chaum (1981) İzlenemez Elektronik Posta, Dönüş Adresleri ve Dijital Takma Adlar başlıklı çalışmasında güvensiz bir iletişim ortamında iletişim kurulan tarafı ve iletişim içeriğini gizlemeyi mümkün kılan, açık anahtarlı şifrelemeye dayalı bir teknik sunmuştur. Sunulan teknik güvenilir bir üçüncü tarafa gereksinim duymamaktadır. Chaum'un (1982) Karşılıklı Olarak Birbirine Güvenmeyen Gruplar Tarafından Kurulan, Sürdürülen ve Güvenilen Bilgisayar Sistemleri konulu doktora tezinde aralarında güven olmayan kuruluşlar arasında yüksek güvenlikli bir bilgisayar sisteminin kurulabileceği öne sürülmüştür. Chaum'un tezinde blokzincirin birçok özelliğine yer verilmiştir. Chaum (1983) İzlenemez Ödemeler İçin Kör İmzalar başlıklı çalışmasında kişinin yaptığı her ödemede, üçüncü bir tarafın, ödemeyi yapan kişinin nerede olduğu, hayat stili gibi birçok bilgiye sahip olabileceğini, nakit ödeme gibi anonim ödeme sistemlerinin ise kontrol ve güvenlik zayıflığı içerdiğini belirterek aşağıdaki özelliklere sahip, kriptografiyi kullanan yeni bir otomatik bir ödeme sistemini önermiştir:

- Üçüncü tarafların ödeme yapılan kişiyi, ödeme zamanını veya yapılan ödemelerin miktarını belirleyememesi,
- Kişinin ödeme yaptığının kanıtını sunabilmesi veya istisnai durumlarda ödeme yapılan tarafın kimliğinin belirlenebilmesi.

David Chaum aynı zamanda dünyanın ilk elektronik ödeme sistemi olarak nitelendirilen DigiCash'in kurucusudur. 1994 yılında Cenevre'de gerçekleştirilen ilk World Wide Web konferansında duyurulan DigiCash, açık anahtarlı kriptografi kullanan, herhangi bir kişisel bilgisayardan diğerine ödeme yapmayı ya da para transfer etmeyi mümkün kılan bir ödeme sistemi olarak duyurulmuştur (Chaum, 1994). 1998 yılında iflas başvurusunda bulunan DigiCash her ne kadar merkezi bir otoriteye bağımlılığı tamamen ortadan kaldırmasa da, kripto para fikrinin temellerini oluşturmuştur.

Bitcoin'den önce, blokzincir benzeri ilk çalışma Stuart Haber ve W. Scott Stornetta tarafından yayınlanmış olan "Dijital bir belgeye nasıl zaman damgası eklenir?" başlıklı çalışmadır. Bitcoin'in duyurulduğu makalenin kaynakları arasında da gösterilen bu çalışmalarında Haber ve Stornetta (1991) belgelerin geriye ya da ileriye doğru tarihlendirilmesi mümkün olmayacak biçimde verilere zaman damgası ekleyen, zaman damgası hizmeti tarafından kayıt tutulmasını gerektirmeden gizliliği koruyan bir prosedür önermektedir. Bitcoin tasarımındaki işlemlerin zaman damgalı olarak kaydedilmesi ve bu kayıtların değiştirilmesinin önlenmesi özelliklerinde bu makaleden faydalanılmıştır. Bitcoin makalesinde zaman damgasına yönelik olarak önerilen tasarıma kaynak gösterilen bir diğer çalışma Bayer, Haber ve Stornetta (1993) tarafından kriptografik hash fonksiyonları ile dijital zaman damgalarının etkinliğinin ve güvenilirliğinin artırılmasında kullanımına ilişkin çözüm önerilen çalışmadır.

Blokzincir teknolojisinin ilk gerçek dünya uygulaması olan Bitcoin'de kullanılan İş İspatı (PoW) mutabakat mekanizmasının ilk ortaya çıkışı 1992 yılında düzenlenen Kriptoloji Konferansında sunulan "İşleme Tabi Tutarak Ücretlendirme veya İstenmeyen E-postalarla Mücadele" başlıklı bildiri ile gerçekleşmiştir. Dwork ve Naor (1993) bu çalışmalarında özellikle önemsiz e-postalarla mücadele etmek ve paylaşılan bir kaynağa erişimi kontrol etmek için bir hesaplama tekniği önermiştir. Bu tekniğin temel fikrini kullanıcının kaynağa erişim için belirli bir zorluk derecesinde hesaplama yapma zorunluluğu oluşturmaktadır.

Böylelikle, çok sayıda istenmeyen e-posta göndermenin göndericiye bir maliyet getirmesi hedeflenmiştir.

Benzer bir mantıkla, bu çalışmadan bağımsız bir biçimde ilk olarak Adam Back tarafından Cypherpunks e-posta grubuna gönderilen bir e-posta mesajı ile duyurulan hashcash adlı mekanizma Bitcoin'de kullanılan İş İspatı mutabakat mekanizmasının temelini oluşturmaktadır. Dwork ve Naor (1993) sonlu bir alanda karekök almak gibi birkaç farklı fonksiyon önermiş, ancak Adam Back çok daha basit bir algoritma ortaya koymuştur. Back (1997) hashcash adını verdiği mekanizma ile aynı anda çok sayıda e-posta gönderimi ile internet kaynaklarının kötüye kullanımına karşı CPU kaynaklarının kullanılması zorunluluğunu getiren bir önlem sunmuştur. Sunulan çözümün temel özellikleri yapılan işin gönderici için makul derecede zor olması, doğrulanmasının kolay olması, az sayıda kişiye gönderilen e-posta mesajlarında kayda değer bir fark yaratmazken çok sayıda kullanıcıya gönderilen mesajlarda göndericiye bir maliyet getirmesidir. Önerilen mekanizma her bir mesaj için mesajın hash değerini almak, ancak bunu yaparken hash değerine belirli bir ön ek getirilmesini zorunlu tutmak biçimindedir. Bu işlem az sayıda mesaj için fark edilmeyecek düzeyde bir işlem zamanı gerektirirken mesaj sayısı arttıkça işlem süresi ve dolayısı ile bilgisayar kaynak kullanımı da kayda değer ölçüde artmaktadır. Back (2002) daha sonraki "Hashcash – Hizmet Reddi (DoS) Saldırısına Karşı Bir Önlem" başlıklı çalışmasında 1997 yılında anonim e-posta gönderiminin sistematik biçimde kötüye kullanımının önlenmesi için önerdiği mekanizmanın farklı uygulamalarından, kazanılan deneyimlerden ve mekanizma için bazı iyileştirmelerden bahsetmektedir.

Bitcoin sisteminde kullanılan "İş İspatı" kavramı terim olarak ilk defa 1999 yılında Markus Jakobsson ve Ari Juels tarafından kullanılmıştır. Jakobsson ve Juels (1999) "İş İspatı ve Ekmek Tatlısı Protokolleri[1]" başlıklı çalışmalarında İş İspatı kavramını resmileştirerek kanıtlayıcı tarafından belirli bir zaman aralığında, belirli bir miktarda hesaplama işinin yapıldığının bir doğrulayıcıya gösterilmesi biçiminde özetlemektedirler.

Temel mantığı ve felsefesi benzer olmakla birlikte yöntemlerinde farklılıklar bulunan bu iş ispatı mekanizmalarından hashcash, dijital paranın erken bir öncüsüdür ve Nakamoto (2008) Bitcoin'i duyurduğu makalesinde Bitcoin'deki iş ispatı uygulamasının ilham kaynağı olarak

[1] Proofs of Work and Bread Pudding Protocols

Adam Back'in hashcash çözümünü göstermektedir. Bitcoin'de kullanılan iş ispatı da işlemi gerçekleştiren tarafından bazı işlerin yapıldığını hesaplama ile kanıtlama sürecidir ve bu hesaplama bir bulmaca aracılığı ile gerçekleşir. Bulmacanın temel özelliği belirtilmesinin kolay, çözmesinin zor, doğrulamasının ise kolay olmasıdır.

Günümüz kripto paralarının temel özelliklerini içeren ve Bitcoin makalesinin referansları arasında yer alan bir diğer çalışma Wei Dai'ye ait "b-money" başlıklı çalışmadır. Dai W. (1998) bu çalışmasında crypto-anarchy hareketine olan hayranlığını vurgulayarak birbirlerine gerçek isimleri ve fiziksel konumları ile bağlı olmayan bir topluluktan, böyle bir topluluğun yaratılabilmesi için gerekli hizmetleri sağlayabilecek izlenemez kuruluşlara olan gereksinimden bahsetmekte, bu kuruluşlar tarafından sağlanacak bir protokol önerilmektedir. İki protokolden oluşan bu öneride gönderici ve alıcıların yalnızca takma adlarla (yani açık anahtarlarla) tanımlandığı izlenemez bir ağ, gönderici tarafından dijital olarak imzalanan ve şifrelenen mesajlar, dışarıdan bir destek almadan anonim taraflar arasında ödeme gerçekleştirilebilmesi ve her takma adın sahip olduğu para miktarını tutan ayrı bir veri tabanı yer almaktadır.

Uygulamadan ziyade kavramsal bir çalışma olan b-money'den kısa bir süre sonra, aynı yıl içinde (1998) Nick Szabo tarafından Bit-Gold yaratılmıştır. Szabo'nun Bit-Gold tasarımında, sistem tarafından atanan kriptografik bir denklemin çözülmesi için katılımcının bilgisayar gücünü tahsis etmesi gerekmektedir. Szabo'ya göre spesifik bir binary dizisi üreten bir iş ispatı fonksiyonu olarak çalışan herhangi bir şey, bu diziyi üretmenin hesaplama açısından maliyetli olduğunu kanıtlayacaktır. Bit-Gold ağında çözülen denklemler topluluğa gönderilmekte, topluluk tarafından çözümün kabul edilmesi halinde ödül, hesaplamayı yapan kişiye verilmektedir. Bu şekilde, her çözüm bir sonraki çalışmanın bir parçası olmakta, bu da büyüyen bir varlık zinciri yaratmaktadır. Bu yaklaşım ağın yeni paraları doğrulayarak zaman damgası ile işaretlemesi için zekice bir yol sağamakta, topluluğun çoğunluğunun çözümleri kabul etmemesi halinde bir sonraki denklemin çözümüne başlanamamaktadır. Dijital para tasarımında en büyük güçlük mükerrer harcama problemidir. David Chaum DigiCash'te bu problemi merkezi otorite ile çözmüştür. Ancak Szabo buna karşı çıkarak güvenilir bir merkezi otoriteye bağımlı olmayan bir çözüm üzerinde çalışmıştır (Peck, 2012). Szabo tarafından tasarlanan ancak uygulamaya geçmeyen Bit-Gold'un temelinde üçüncü taraflara minimum bağımlılıkla çevrimiçi ve belirli bir maliyete katlanılarak yaratılan bitler, bunların depolanması, aktarılması ve minimum güven

gereksinimi ile analiz edilebilmesi yatmaktadır. Szabo (2005) hayal ettiği Bit-Gold'u detaylı biçimde tarif ettiği yazısında hemen hemen Bitcoin ile aynı biçimde işleyen bir sistem ortaya koymuş, ancak çifte harcama problemine merkezsiz bir çözüm getirememiştir.

Yukarıda sıralanmış olan çalışmaların yanı sıra, kuşkusuz Bitcoin özelinde blokzincir teknolojisinin yaratılmasında en büyük rol şifre anarşistleri (Cypherpunks) olarak bilinen bir grubun e-posta gruplarında yaptıkları yazışmalardır. Güven ve Şahinöz (2018: 141) blokzincir teknolojisinin meydana getirdiği dönüşümü Avusturya asıllı Amerikalı iktisatçı J. A. Schumpeter'in "her yeni icat yapıcı bir yıkıcılık barındırır" sözüne atıfla yaratıcı yıkım olarak tanımlamakta, kripto para, blokzincir teknoloji devrimi ve Bitcoin konusunda konuşulan ne varsa Cypherpunks adıyla bilinen bir avuç aktivist ile başladığını ileri sürmektedir.

Temelleri bireylerin mahremiyetinin önemine, devletler başta olmak üzere tüm otoritelerin bu mahremiyeti ihlal etmelerine karşı önlem almaya dayanan bu hareket ilk olarak 1992 yılının sonlarında Timothy C. May, Eric Hughes ve John Gilmore öncülüğünde başlatılmıştır. Dünya devletlerinin internet üzerinden yaptıkları izleme ile bireylerin mahremiyetlerini ve özgürlüklerini yok ettiğini düşünen grup üyeleri bilgisayarlar, matematik ve fizik ile bireysel özgürlüğün korunabileceğini öne sürmektedir. Başlangıçta küçük bir grup olarak belirli aralıklarla bir araya gelen gruba Jude Milhon tarafından Cypherpunks adı verilmiştir (Bartlett, 2016: 86, 87). Grubun büyümesiyle bir e-posta listesi oluşturulmasına karar verilmiş, bu e-posta listesinde yer alan isimlerin sayısı 1994'te 700'e, 1997'de ise 2 000'e ulaşmıştır. Grubun kurucularından Hughes (1993) yayınladığı "Bir Şifre Anarşistinin Manifestosu" başlıklı manifesto ile Cypherpunks'ın temel felsefesini duyurmuştur. Bu manifestoda özetle elektronik çağda açık bir toplum için mahremiyet gerektiği, mahremiyet ile gizliliğin aynı şey olmadığı, mahremiyetin kişinin bilgilerini kendi istedikleri ile paylaşabilme gücü olduğu, bu mahremiyetin de yasalarla değil fizik ve matematik ile sağlanabileceği, devletler, şirketler ya da büyük kuruluşlardan halkın mahremiyetini korumalarının beklenemeyeceğini vurgulamıştır. Cypherpunks'a göre halk kendi mahremiyetini kendi korumalıdır. Bunun sağlanması için de gerekli olan yazılımları grubun kendisi geliştirecek, mahremiyet kriptografi, anonim posta yönlendirme sistemleri, dijital imzalar ve elektronik para ile savunulacaktır. Cypherpunks grubu yayınlamış oldukları manifestolarında da açıkça belirtmiş oldukları üzere, iletişimde ve verinin muhafazasında mahremiyetin yasalarla değil fizik ve matematik ile sağlanabileceğini öne

sürmekte ve bu nedenle devletlerin kriptografi kullanımı konusunda getirmek istediği kısıtlamalara şiddetle karşı çıkmaktadır.

Cypherpunks, kriptografinin ve şifrelemenin siber uzayda mahremiyeti korumak için yeterli olmadığını, tamamen özgür dijital bir toplum için tamamen egemen bir ekonomiye, dolayısı ile dijital bir paraya gerek olduğunu da öne sürmektedir. May (1994) "Kripto Anarşi ve Sanal Toplumlar" başlıklı yayınında dijital para, şifreleme, dijital imzalar, dijital karıştırıcılar (yeniden e-posta gönderimi) ve ilgili teknolojileri içeren Güçlü Kripto ile ağlar, anonim iletişim, metin esaslı çevrimiçi sanal gerçeklik sistemi olan MUD (Multi-User Domain) ve MOO (MUD Object Oriented) ve çoklu evren tarzı sanal gerçeklikleri içeren Siberuzay Toplulukları olmak üzere iki ana teknolojinin bir kombinasyonunu detaylı biçimde tarif etmektedir. May'e (1994) göre Cypherpunks grubu bahsedilen sanal toplum için oldukça iyi bir örnektir. Dünyanın dört bir yanına dağılmış, dakikalar içinde elektronik olarak iletişim kuran ve yerel yasalara aldırış etmeyen Cypherpunk'lar gerçekten sanal bir topluluktur. Çoğu üye takma adlar kullanır ve listedeki diğer üyelerle iletişim kurmak için anonim e-posta göndericiler kullanırlar. Listenin kendisi böylece, her türden bilginin anonim olarak saklanabileceği ve anonim olarak alındığı bir mesaj havuzu işlevi görmektedir.

İçerisinde matematik, kriptoloji, bilgisayar bilimleri, politika ve felsefe gibi konularda teknik tartışmaların yürütüldüğü çok aktif bir forum platformu işlevi gören Cypherpunks'un üyeleri içinde Bitcoin'in yaratıcısı Satoshi Nakamoto, Wikileaks'in kurucusu Julian Assange, Tor geliştiricisi Jacob Appelbaum, hashcash çözümünün mimarı Adam Back, BitTorrent'in kurucusu Bram Cohen, Yeniden Kullanılabilir İş İspatı'nın yaratıcısı ve PGP 2.0'ın (Pretty Good Privacy – güvenli iletişim için bir şifreleme ve anahtar değişimi yazılımı) ana yazılımcılarından Hal Finney, OpenSSL'in öncüsü olan SSLeay'ın yazarlarından Tim Hudson, SSL 3.0'ın yazarlarından Paul Kocher, PGP 1.0'ın yaratıcısı Philip Zimmermann, b-money'in kurucusu Wei Dai, Bell Labs araştırmacılarından Steven Bellovin ve Matt Blaze, GNU Radio projesinin kurucusu ve kriptografik olarak güvenliği sağlanmış Starium mobil telefonunun tasarımcısı Eric Blossom, OpenPGP'nin teknik liderlerinden Jon Callas, inkar edilebilir kriptografinin mucitlerinden Suelette Dreyfus, Bitcoin'in öncülerinden BitGold'un yaratıcısı ve akıllı sözleşme kavramının mucidi Nick Szabo, Zcash'in kurucusu, DigiCash'in geliştiricisi Zooko Wilcox-O'Hearn, SSL'in mucidi ve Netscape'in kurucularından biri olan Marc Andreessen gibi birçok ünlü isim bulunmaktadır. Bitcoin ilk olarak Cypherpunks e-posta grubuna gönderilen bir posta ile duyurulmuştur.

1996 yılında Dr. Douglas Jackson tarafından kurulan E-Gold, Bitcoin'den önceki dijital para fikrinin öncülerinden biridir. Altın destekli dijital bir sistem sunan E-Gold dünyanın herhangi bir yerindeki bir insanın herhangi bir banka hesabına ihtiyaç duymadan, çok düşük bir ücretle para transferi yapmasına olanak sağlamıştır. E-Gold ödeme aracı olarak kullanılabilen, internet işlemleri için özel olarak tasarlanmış olan, hesap bakiyelerini gram saf altın olarak Londra'da tutan, sadece birkaç fare tıklaması ile hesap açılabilen, kullanıcıların sahte ad kullanılabildiği bir sistem olarak tarif edilmektedir. Kredi kartı ya da banka havalesi ile e-altın birimleri satın alınarak yine e-altın hesabı bulunan başka birine bu birimler aktarılabilmektedir. 2005 yılında 1,2 milyon hesap ve 1,5 milyar $ işlem hacmine sahip olan E-Gold çevrim içi ödeme sektöründe PayPal'in ardından ikinci sıraya kadar yükselmiştir. 2005 yılında kredi kartı dolandırıcılarının haksız kazançla elde ettikleri fonları transfer etmek için E-Gold'u kullanmaları gerekçesi ile FBI tarafından baskına uğrayan firma, Adalet Bakanlığı'nın ve finansal düzenleme kuruluşlarının kara para aklama, lisanssız para transferi işlemleri gerçekleştirme suçlamalarına maruz kalmış, on yıldan fazla hapis cezası ve milyarlarca dolar ceza ile tehdit edildikten sonra yapılan savunma pazarlığı sonucunda Jackson altı aylık ev hapsi ve elektronik izleme, 36 aylık denetimli serbestlik cezasına çarptırılmış, yaklaşık 1,2 milyon $ hükumete teslim edilmiş, firmalarına 300 bin $'lık para cezası kesilmiştir. Yine anlaşmaya göre müşterilerinin kimliklerinin doğrulanması, şüpheli faaliyetlerin raporlanması, ABD Gelir İdaresi Banka Gizlilik Yasası Birimi'nin düzenli denetimine tabi olması koşullarına uygun hale gelinceye kadar E-Gold'un hizmetleri durdurulmuş, daha sonra da tekrar hizmet vermeye başlamamıştır (White, 2014). E-Gold'un merkezi yapıda olması ve altın gibi fiziksel bir varlıkla desteklenmesi kendisini hükumete karşı savunmasız hale getirmiştir.

Bitcoin tarihinde en önemli yer tutan isimlerden biri de Hal Finney'dir. Satoshi Nakamoto'nun ilk Bitcoin transferini gerçekleştirdiği isim olmasının ötesinde kriptografi konusunda önde gelen bir isim, bir Bitcoin madencisi ve Yeniden Kullanılabilir İş İspatının (RPOW) geliştiricisidir. Finney (2004) 2004 yılında Cypherpunks e-posta grubuna gönderdiği mesaj ile duyurduğu RPOW sisteminin bir iş ispatı tokeni olarak hashcash'i aldığını ve karşılığında RPOW tokenleri olarak adlandırdığı RSA imzalı tokenlar yarattığını belirtmiştir. RPOW sistemi temelinde İş İspatı jetonunun bir defa kullanılmasına, ardından yeni bir jetonla değiştirmesine dayanmakta olup çalışma sistemi Bitcoin ile çok yakındır.

Birçok keşif ya da yenilik gibi, Bitcoin de kendisinden önce yapılmış olan çalışmaların üzerine bina edilmiş, merkezsiz bir dijital para tasarımındaki farklı problemlere getirilen çözümleri bir araya getirip kendisinden önceki çalışmalarda giderilememiş olan mükerrer harcama problemini de çözerek neredeyse kusursuz bir tasarım sunmuştur. Adından da anlaşılacağı üzere, mükerrer harcama aynı paranın iki defa harcanmasıdır. Geleneksel finansal sistemde bu sorunun çözümü için bankalar gibi merkezi kurumlara ihtiyaç duyulmaktadır. Bitcoin'e kadar herhangi bir merkez ya da güvenilir üçüncü taraf olmadan bu soruna çözüm getirilememiştir.

Birbirine güvenmeyen taraflar arasında güvenli bir iletişimin sağlanması problemi Bizanslı Generallerin Problemi olarak Lamport, Shostak ve Pease (1982) tarafından dile getirilmiştir. Tarif edilen sorun, bilgisayar sistemlerinin farklı bileşenlerden gelen çelişkili bilgileri işlemesi ile ilgili olup bilgisayarın ya da ağın, birbirleri ile çelişen bilgiler aldığında hangi bilginin doğru olduğuna nasıl karar vereceğine ilişkindir. Bitcoin işte bu sorunu hashcash'ten esinlenen ve hashcash tasarımını ağdaki eş düğümler arasındaki bir iş ispatı mutabakat mekanizması ile birleştiren bir çözümle gidermiştir.

Bitcoin isimi ilk defa 2008 yılının 18 Ağustos tarihinde anonim olarak alan adı kaydı yapılmasına izin veren bir alan adı sağlayıcısı olan "anonymousspeech.com" sitesinden "Bitcoin.org" alan adı kaydı ile ortaya çıkmıştır (Bitcoin.org, 2014). Ardından, 31 Ekim 2008 tarihinde Satoshi Nakamoto kullanıcı adı ile "metzdowd.com" kriptografi e-posta grubuna "Bitcoin P2P e-cash paper" konu başlığı ile bir e-posta mesajı gönderilmiş, bu mesajda tamamen eşten eşe ve güvenilir bir üçüncü tarafa ihtiyaç duymayan yeni bir elektronik para sistemi üzerinde çalışıldığı belirtilerek halen erişilebilir olan http://www.bitcoin.org/bitcoin.pdf adresinden bu çalışmanın makalesine ulaşılabileceği bilgisi verilmiştir (Nakamoto, 2008a). 9 Kasım 2008 tarihinde Bitcoin projesi açık kaynak kodlu yazılım geliştirme platformu olan SourceForge.net'e kaydedilmiş, 3 Ocak 2009 tarihinde de Genesis block olarak adlandırılan Bitcoin'in ilk bloğu Satoshi Nakamoto tarafından yaratılmıştır. 9 Ocak 2009 tarihindeyse Microsoft Visual Studio ile derlenmiş olan Bitcoin Version 0.1 sürümü yayınlanarak 12 Ocak 2009'da Hal Finney'e 170. Bitcoin bloğu içerisinde ilk transfer gerçekleştirilmiştir. 5 Ekim 2009 tarihinde Bitcoin üreten bir bilgisayarın harcadığı elektriğin maliyetini içeren bir denklem kullanılarak New Liberty Standard tarafından Bitcoin'in değeri ilk defa bir kur olarak yayınlanmıştır. Bu ilk değerlemeye göre 1 $'ın karşılığı 1 309 BTC olarak belirlenmiştir. 12 Ekim 2009 tarihinde

açık kaynak kodlu yazılım geliştirme topluluklarının tartışma platfomu olan freenode IRC'de #bitcoin-dev adlı bir kanal kaydı yapılmış, 16 Aralık 2009'da Bitcoin Sürüm 0.2 yayınlanmış, 6 Şubat 2010 tarihinde de dwdollar tarafından ilk Bitcoin alım-satım borsası kurulmuştur. 22 Mayıs 2010 tarihinde Bitcoin kullanılan ilk gerçek dünya işlemi gerçekleştirilmiş, bir programcı olan Laszlo Hanyecz tarafından 25 $ değerindeki bir pizza için 10 000 Bitcoin ödenmiştir. 11 Temmuz 2010 tarihinde ünlü bilgisayar ve teknoloji sistesi slashdot.org'da Bitcoin v0.3'ten bahsedilmesini takiben birçok yeni kullanıcı Bitcoin ağına dahil olmuş, birkaç gün içinde Bitcoin'in değeri on kat artmıştır. 17 Temmuz 2010 tarihinde Jed McCaleb tarafından ünlü kriptopara borsası MtGox kurulmuş, Bitcoin sistemindeki blokların uygun olmayan biçimde doğrulanmasına neden olan bir zafiyet sonucunda 15 Ağustos 2010 tarihinde 74 638 numaralı blokta 184 milyar BTC üretilmiştir. Zafiyetin hemen farkedilmesiyle, Satoshi Nakamoto ve Gavin Andresen tarafından koddaki zafiyet için bir yama yayınlanmış, bu noktada blokzincirde bir çatallanma meydana gelmiştir. İki zincir halinde bir süre devam eden Bitcoin blokzinciri 74 691 numaralı blokta doğru olan çatallanmanın hatalı olanın uzunluğunu geçmesi ile, işlemlerin her zaman en uzun zinciri takip etmesi kuralına göre bu zincirden işlemlere devam etmiştir. En uzun zincirden devam eden Bitcoin blokzincirde bu nedenle o hatalı yaratılan Bitcoinler mevcut değildir. 2010 yılı Ekim ayında kara paranın aklanmasının ve terörün finansmanının önlenmesi için politikalar geliştiren hükumetlerarası bir kuruluş olan Mali Eylem Görev Gücü (TATF) tarafından dijital para birimlerinin terörist grupları desteklemek için kullanımı konusunda bir uyarı yayınlanmıştır. Bitcoin'in piyasa değeri ilk defa 6 Kasım 2010 tarihinde 1 milyon $'ı aşmıştır (Bitcoin.org, 2014).

2009 yılında ilk bloğun yaratılmasıyla faaliyetine başlayan Bitcoin sistemi o zamandan bu yana sıfır kesinti ile çalışmış, sisteme hiç ara verilmemiş, dokuz sayfalık bir teknik açıklama belgesinden piyasa değeri milyarlarca $ olan bir kriptopara birimi, yaklaşık bir trilyon $'lık bir kriptopara piyasası, muazzam büyüklükte bir bilgisayar ağı, birçok kod geliştirici, kullanıcı, yatırımcı ve firmalardan oluşan büyük bir ekosistem ortaya çıkmıştır.

2.1.2. Blokzincirin çalışma prensibi – Bitcoin örneği

Her ne kadar blokzincir teknolojisinin mimarı olarak Satoshi Nakamoto gösterilse de, aslında Bitcoin'in ilk olarak duyurulduğu çalışmada blokzincir terimi hiç kullanılmamıştır. Bu yayında geçen, blokzincir terimine en yakın ifade 'blokların zinciri – *chain of blocks*'

ifadesidir. Blokzincir kavramı Bitcoin'den çok daha geniş bir alanı kapsamakla birlikte, blokzincir teknolojisinin ilk gerçek dünya uygulaması olması nedeni ile Bitcoin'in anlaşılması, blokzincir teknolojisinin anlaşılması bakımından önemlidir.

Nakamoto (2008a) ilk olarak duyurduğu çalışmasında Bitcoin'i herhangi bir finansal kuruluşun aracılığına gereksinim duyulmadan iki taraf arasında çevrim içi ödemeyi mümkün kılan, tamamen eşten eşe bir elektronik para olarak tanımlamıştır. Yine bu çalışmada, sistemin temel özellikleri aşağıdaki biçimde sıralanmıştır:

- Güvenilir bir üçüncü taraf olmaksızın doğrudan işlem yapabilme,
- Geriye döndürülemez (silinemez ve değiştirilemez) işlemleri gerçekleştirebilme,
- İşlem ücretlerini azaltma,
- Çifte (mükerrer) harcamayı engelleme,
- Kullanıcıların anonimliğini sağlama.

Bitcoin, Satoshi Nakamoto'nun makalesinin ilk bölümünde yer verdiği bazı mevcut sistem problemlerine bir çözüm getirmek üzere geliştirilmiştir. Mevcut sistemdeki bu problemler ve Bitcoin'in çözüm aradığı konular aşağıdaki biçimdedir:

- Mevcut sistemde nakit kullanılarak yapılan işlemler dışındaki işlemlerde, yani elektronik ödeme ve transfer işlemlerinde güvenilir üçüncü taraflar bulunması zorunludur. Güvenilir üçüncü taraflarla ilgili problemler ise aşağıdaki biçimdedir:
  - Geriye dönüşü olmayan işlemler mümkün değildir. Yani, işlemi gerçekleştiren taraflardan bağımsız biçimde, üçüncü taraflarca işlemlerde değişiklik yapılabilir, ya da istenen kayıtlar yok edilebilir.
  - Aracılık hizmetlerinin getirdiği bir maliyet bulunmaktadır ve bu maliyet işlem ücreti olarak işlem gerçekleştirilenlere yansıtılmaktadır.
  - Mikro ya da nano ödeme olarak adlandırılan çok küçük tutarlı ödemeler gerçekleştirilememektedir.
  - İşlemleri gerçekleştirebilmek için aracılarla ihtiyaç duyulan bilgilerden daha fazlasının paylaşılması gerekmektedir.
  - Aracılar merkezi yapıdadır ve saldırılara ve tek nokta hatasına açıktır. Bu riskleri yönetmek için büyük güvenlik ve iş sürekliliği yatırımı gerekmektedir.
- Dünya üzerinde kimliği, banka hesabı bulunmayan, finansal sisteme dahil olmayan bir milyardan fazla insan bulunmaktadır. Bu insanların mevcut sistemde finansal işlem

yapmaları olanaksız, mevcut sistem üzerinden yapılan yardımlara ulaşmaları çok güçtür.

- Uluslararası transferler için bekleme süreleri çok uzundur. SWIFT sistemi üzerinden yapılan ödemeler üç ila beş gün, bazı durumlarda çok daha uzun sürebilmektedir.
- Mevcut sistemde mesai saatleri dışında transfer gerçekleştirilememektedir.
- Aracıların sağladıkları güven karşılığında paylaşılan bilgiler başta teknoloji devleri olmak üzere tüm aracılarca kazanca çevrilmekte, verinin sahibinin mahremiyeti ihlal edilirken bunun yanı sıra bu bilgiler farklı amaçlarla kullanılabilmektedir.

Bitcoin ile ortaya konulan sistem sayılan bu sorunların üstesinden gelmek ve yepyeni bir elektronik ödeme sistemi yaratmak için aşağıdakileri kullanmaktadır:

- Dijital imza: Bitcoin sisteminde elektronik para bir dijital imza zinciri olarak tanımlanmaktadır. Blokzincir teknolojisinde şifreleme ve şifreyi çözmek için farklı anahtarların kullanıldığı açık anahtarlı kriptografi kullanılmaktadır. Bitcoin transferinde gönderici kendi dijital imzası ile bir önceki işlemin hash değerini ve alıcının açık anahtarını imzalar.
- Açık Anahtar Altyapısı: Açık anahtarlı şifrelemede bir açık bir de özel anahtar olmak üzere bir anahtar çifti kullanılır. Açık anahtarın açığa çıkması özel anahtarı tehlikeye atmaz, ancak özel anahtar gizli tutulmalıdır. Bu teknik sadece güvenli olmayan açık bir ağda güvenli iletişime izin vermekle kalmaz, aynı zamanda dijital imzalar aracılığı ile kimlik doğrulamayı da destekler. Açık Anahtar Altyapısı dijital imzaları oluşturan, depolayan, dağıtan, iptal eden ve silen, yani dijital sertifikaları işleyen bir sistemdir. Bir kayıt işlemiyle doğrulanan bir kimliği ortak anahtarla bağlar, bir Sertifika Yetkilisi (CA) tarafından imzalanan ve teslim edilen bir sertifika verir. Böylelikle, bir sertifikada bir tanımlayıcı, bir açık anahtar ve bir dijital imza bulunur. Açık Anahtar Altyapısı güvenilir bir üçüncü taraf (CA) aracılığıyla bir kimliği açık anahtara bağlayarak güçlü kimlik doğrulamayı kolaylaştırır. Açık Anahtar Altyapısı blokzincir sistemlerinde işlem oluşturma ve doğrulama sürecinde temel bir bileşen olarak yer alır. Benzer biçimde özel ve izin gerektiren blokzincirde dijital imzalar düğümlerin önceden seçilmesi, blokzincirdeki işlemlerin doğrulanması ve işlemlerin saklanmasında kullanılabilmektedir.
- Kriptografi: Güvenilir bir üçüncü taraf olmadan birbirlerine güvenmeyen iki taraf arasında gerek duyulan güven mekanizmasının sağlanması için kullanılır. Açık

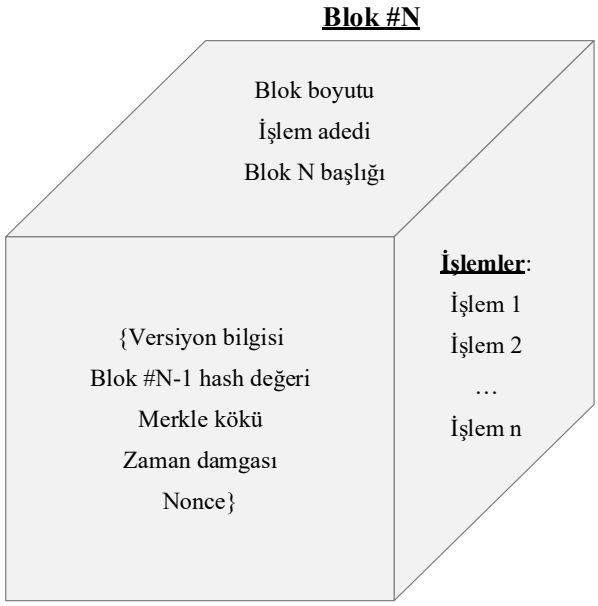
anahtarlı kiptografi ile anonimlik sağlanır. Tek tek her işlemin zamanı ve miktarı herkesin görebileceği biçimde ilan edilmek ancak gönderici ve alıcının kimlikleri yerine açık anahtarları kullanılmaktadır. Açık anahtarın sahibi ile ilişkisini gizlemek için her işlemde yeni bir anahtar çifti kullanılır.

- Hash fonksiyonu: İş ispatı mekanizmasının işletilmesinde ve blokların birbirine bağlanmasında kullanılır. Bitcoin'de hash fonksiyonu olarak SHA256 kullanılmaktadır.
- Merkle ağacı: Blokların içinde yer alan işlemlerin doğrulanmasını, tek tek tüm işlemlerin kontrol edilmesine gerek duyulmadan sağlar. Paranın kullanıldığı son işlem yeterli sayıda bloğun altında kaldığında, saklama alanından tasarruf etmek için öncesindeki harcama işlemleri silinebilirler. Bloğun hash değerini bozmadan bunu saklamak için işlemler bir Merkle ağacında tutulur ve sadece Merkle kökü blok hash değerine dâhil edilir. Eski bloklar ağaç dalları budanarak sıkıştırılabilir.
- Eşten eşe (P2P) ağ: Çifte (mükerrer) harcama probleminin giderilmesi için, İş İspatı mutabakatında kullanılır. Bitcoin ağı eşit önceliğe sahip bilgisayarlardan oluşur ve bu ağ herkese açıktır. Bu bilgisayarlar hem sunucu hem de istemci işlevi görebilmektedir.
- Zaman damgası: İşlemlerin birbiri ardına eklenmesi ve daha sonra değiştirilmesinin hemen hemen imkânsız hale getirilmesi için hash fonksiyonuna dayalı bir iş ispatı mekanizması ve zaman damgası kullanılır.
- Oyun teorisi: Sistem, ağdaki düğümlerin çoğunluğu ya da bir başka ifade ile ağdaki toplam CPU gücünün çoğunluğu kötü niyetli olmadıkça en uzun (doğru) zincirin takip edilerek saldırganların alt edilmesini sağlayacak biçimde kurgulanmıştır. Saldırganın, bütün dürüst düğümlerden daha fazla işlem gücünü toplamayı başarması halinde ödemeleri çalarak insanları dolandırmayı seçmesi halinde kazancı kurallara uyması halinde kazanacağından daha az olacaktır. Temel olarak; kurallara uymanın kişiler için en uygun seçenek olduğu, topluluk menfaatlerinin kişisel menfaatleri optimize ettiği bir sistem kurgulanmıştır. Bitcoin sistemi içerisindeki ödül mekanizması da katılımcıları kurallara uymaya teşvik etmektedir. Bitcoin işlemlerini gerçekleştirmek için harcanmak zorunda olan CPU ve elektrik nedeniyle sistem içerisindeki kötü niyetli aktörlerin parasal bir kayıp yaşayarak cezalandırılmaları oldukça olasıdır. Oyun teorisinin Nash dengesi, Schelling odak noktası ve Grimm tetiği konuları blokzincir mimarisinde hayat bulmaktadır.
- Olasılık teorisi: Sistem, dürüst düğümler topluca saldırgan düğümlerden daha fazla CPU gücünü ellerinde bulundurduğu sürece güvenlidir. Kumarbazın iflası problemine

benzer biçimde, Bitcoin sistemine saldıran bir saldırganın yakalamak zorunda kaldığı blok sayısı arttıkça başarı olasılığı üstel olarak azalmaktadır. Alıcı ile gönderici arasındaki hileli işlem olasılığı da aynı biçimde Poisson dağılımına uygun olarak blok sayısı arttıkça katlanarak azalmaktadır.

Bitcoin özelinde blokzincirin çalışma prensibinin anlaşılması için öncelikle bazı terim ve kavramların açıklanması gerekmektedir. Bu terim ve kavramlar aşağıda maddeler halinde özetlenmiştir:

- Adres: Bitcoin ağında ödeme yapmak ve ödeme almak için kullanılan alfanümerik karakterler bütününe verilen isimdir. Taranabilir bir QR kod olarak da kullanılabilir. Bitcoin'le ödeme alınabilmesi için ödeme yapacak tarafa verilmesi gereken tek bilgidir. Bitcoin'de her işlem için ayrı ve benzersiz bir adres kullanılır.
- Blok: Blokzincirde işlem kayıtlarının metadata bilgisi ile birlikte tutulduğu kayıttır. İşlem kayıtları blok içerisinde kaydedildikten sonra değiştirilemez ve silinemezler. Bu blok yapıları bir zincir şeklinde (zaman açısından doğrusal bir dizi yapısında) düzenlenir. Bitcoin'de yaklaşık her on dakikada bir yeni bir blok madencilik yoluyla blokzincire eklenir. Bir bloğu tanımlamanın blok hash değeri ve blok yüksekliği olmak üzere iki yolu vardır. İlk blok yüksekliği sıfırdır ve takip eden her blok ardışık olarak artan yükseklik değerine sahiptir. İlk blok genesis (başlangıç) blok olarak adlandırılır. Bitcoin sistemindeki blok yapısı Şekil 2.3'te verilmiştir.



Şekil 2.3. Bitcoin sisteminde blok yapısı

Şekil 2.3'te verilmiş olan blok içeriğinin veri boyutu ile bu alanlara ilişkin açıklamalar Çizelge 2.1'te gösterilmektedir:

Çizelge 2.1. Bitcoin sistemindeki blok içeriği

Alan	Boyut	Açıklama
Özel sayı	**4 byte**	«Aşağıdaki ifade bir bloktur» anlamında bir ifadedir (Her zaman 0xD9B4BEF9'dur).
Blok Boyutu	**4 byte**	Bu alanı takip eden, byte cinsinden bloğun boyutunu ifade etmektedir
Blok Başlığı	**80 byte**	Blok başlığı birçok farklı alandan oluşmaktadır. Bu alanlar Çizelge 2.2'de verilmektedir.
İşlem Sayacı	**1-9 byte**	Takip eden işlemlerin sayısını ifade etmektedir.
İşlemler (transaction)	**Değişken**	Bu blokta kaydedilmiş olan işlemlerin listesidir.

Çizelge 2.1'de verilmiş olan Blok Başlığının içerdiği alanlar Çizelge 2.2'de verilmektedir.

Çizelge 2.2. Bitcoin blok başlığının içerdiği veriler

Alan	Boyut	Açıklama
Versiyon	**4 byte**	Yazılım/protokol güncellemelerini izlemek için versiyon numarasıdır.
Önceki bloğun hash değeri	**32 byte**	Zincirdeki önceki bloğun (parent) hash referansıdır.
Merkle kökü	**32 byte**	Bu bloktaki işlemlerin Merkle ağacının kökünün hash değeridir.
Zaman damgası	**4 byte**	Bloğun yaklaşık yaratılma zamanıdır (Unix Epoch saniye).
Zorluk	**4 byte**	Bu blok için İş İspatı algoritması zorluk hedefidir.
Nonce değeri	**4 byte**	İş İspatı için kullanılan sayaç benzeri değişkendir.

- Blok ödülü: Başarılı bir biçimde blok oluşturan madenciye verilen belirli miktardaki Bitcoin'dir. Hem Bitcoin sisteminin teşvik mekanizması hem de yeni para basılmasına benzer biçimde yeni Bitcoin yaratılmasının tek yoludur. Bitcoin'in ilk olarak işlemeye başladığı 2009 yılında 50 BTC olan bu ödül miktarı her 210 bin blokta yani yaklaşık dört yılda bir yarıya düşmekte, bu işleme halving adı verilmektedir. Bitcoin sisteminde ilk yarılanma 28 Kasım 2012'de gerçekleşmiş, blok ödülü 25 BTC'ye düşmüştür. Benzer biçimde 9 Temmuz 2016 yılında ikinci yarılanma ile ödül 12,5 BTC'ye, 12 Mayıs 2020 tarihindeki son yarılanma ile 6,25 BTC'ye düşmüştür. Bu kurgu ile aynı zamanda Bitcoin'in arz miktarı kısıtlanmış olup bu arz 21 milyondur. 21 milyon olarak belirlenmiş olan maksimum arz miktarına 2140 yılında ulaşılacaktır.

- Düğüm: Bitcoin ağına bağlı her bilgisayar düğüm olarak adlandırılmaktadır. Bitcoin blokzinciri kendi bilgisayarında tutan bilgisayarlara ise tam düğüm (full node) adı verilmektedir.
- Madencilik: Bilgisayar donanımı kullanılarak, şifrelenmiş problemleri çözerek hem işlemlerin doğrulanması hem de yeni Bitcoinler üretme eylemidir. Madencilik, bir transfer işlemindeki 'nonce' (number only used once) değerinin bulunması sonucunda işlemin blokzincire eklenmesidir. Nonce bir SHA256 değeridir ve "*sha256(transactions, prev_block_hash, nonce) < t"* formülüne uygun olarak tahmin edilmeye çalışılır. Burada 't' değeri birkaç sıfır ile başlayan bir eşik değeri temsil etmektedir. Bu değer Bitcoin ağındaki katılımcıların hesaplama gücüne göre ayarlanmaktadır. Bu formülü çözmek zor, doğrulaması ise kolaydır.
- Zorluk: Bitcoin sisteminde bir bloğun oluşturulması için çözülmesi gereken bulmacanın bir başka ifade ile hedefin altında hash değerini bulmanın ne kadar zor olduğunun ölçüsüdür. Zorluk değeri arttıkça aynı miktarda blok üretmek için gerekli işlem gücü artar. Bitcoin sisteminde zorluk değeri blok üretim zamanını on dakika civarında tutacak biçimde ayarlanmaktadır. Her 2 016 blokta (yaklaşık iki haftada) bir blokların zaman damgaları karşılaştırılarak 2 016 bloğu üretmek için geçen zaman hesaplanır (T). 2 016 bloğun üretilmesi için iki hafta süre geçmesi istenmektedir. Eğer bulunan T değeri bundan farklıysa zorluk değeri "2 hafta/T" değeri ile çarpılır. Böylelikle blok yaratma süresinin 10 dakikayı aşması halinde zorluk derecesi düşürülmekte, aksi durumda zorluk artırılmaktadır.
- Mutabakat mekanizması: Ağ üzerindeki tüm makinelerde blokzincir ağındaki verinin eşlenik bir kopyasının bulunmasını sağlamak için ağ genelinde mutabakat (konsensüs) sağlanması gerekir. Bunu sağlamak için kriptografik hash ve zaman bilgisi kullanılmaktadır.
- Hash: Değişken bir miktarda veri alan ve daha kısa, sabit uzunlukta bir çıktı üreten matematik işlemidir. Hash bir şifreleme işlemi değil, mesajın doğruluğu ya da veri bütünlüğünün kontrolü, dijital imza, kimlik doğrulama, veri bozulmasının kontrolü gibi çok geniş kullanım alanı olan bir matematiksel fonksiyondur. Temel özellikleri tek yönlü bir fonksiyon olması, çıktıyı kullanarak girdiyi bulmanın hemen hemen imkânsız olması, girdinin boyutuna bağlı olmaksızın çıktının hep aynı boyutta olması, girdideki en küçük bir değişikliğin neredeyse tamamen farklı bir çıktı üretmesi (çığ etkisi), bulmasının çok zor doğrulamasının ise çok kolay olmasıdır. Hash dijital parmak izine benzetilebilir.

Bitcoin blokzincirde hash, blokların birbirine bağlanmasında, madencilik sürecinde, işlemlerin ve blokların tasdik edilmesi ve doğrulanmasında ve dijital imzada kullanılır. Hash fonksiyonlarının blokzincir dışında da pek çok kullanım alanı bulunmaktadır.

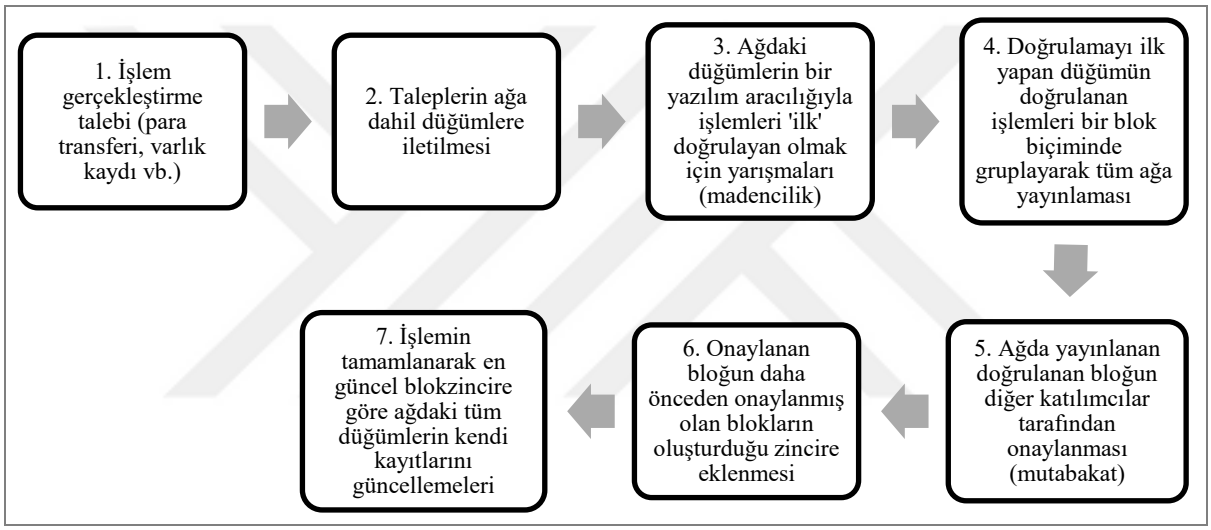
- Nonce değeri; Değeri madenciler tarafından bulunmaya çalışılan, 32-bitlik (4-byte) bir alandır. Bir blok için doğru olarak bulunan nonce değeri yalnızca o blok için geçerlidir (tek kullanımlıktır). Blok içerisinde yapılacak en küçük bir değişiklik, hash fonksiyonunun çığ etkisi özelliği nedeniyle nonce değerini geçersiz hale getirecektir.

Yukarıda açıklanmış olan kavramların tamamı Bitcoin sisteminin işletilmesinde, herhangi bir üçüncü tarafın aracılığına ihtiyaç duyulmadan, anonim bir biçimde transfer işlemlerinin gerçekleştirilmesinde, gerçekleştirilen işlemlerin geri döndürülemez biçimde kaydedilmesinde, işlemler doğrulanırken aynı zamanda Bitcoin arzının, yani sisteme yeni Bitcoinlerin arz edilmesinde ve tüm bu kayıtların güncel biçimde birçok düğümde tutulmasında kullanılmaktadır. Bitcoin'in çalışma prensibi aşağıda maddeler halinde özetlenmiş, ayrıca Şekil 2.4'te gösterilmiştir:

1. İlk adım, iki taraf arasında gerçekleşen bir işlem talebi ile başlamaktadır. Bitcoin sisteminde, bir işlem talimatı gönderildiği anda bu işlem gerçekleşmez. Tüm işlem talepleri öncelikle bir işlem havuzunda (ya da bellek havuzu) tutulur. Bu havuzda sürekli olarak biriken işlem talepleri içerisinden blok kapasitesini aşmayacak sayıda işlem madenciler tarafından blok oluşturmak üzere seçilir.
2. Önceki bloğun hash değeri, seçilen işlemler, bloğa ait metadata verisi (işlem adedi, blok yüksekliği, blok başlığı, zaman damgası gibi) ile aday blok oluşturulur. Madenci, kazanması halinde elde edeceği ödülü de bir işlem olarak işlemler listesine ekler. Aday blok içerisinde ayrıca işlemlerin hash değerlerinin ikili birleştirilmesi ile elde edilen Merkle kök değeri de yer alır.
3. Sistemin belirlediği zorluk derecesine bağlı blok hash değerini bulmak, yani genel bilinen ifadesi ile sistemin sorduğu bulmacayı çözmek için tüm bu verilere nonce değeri ilave edilerek blok hash değeri hesaplanır. Hedef hash değeri elde edilene kadar nonce değeri değiştirilerek bloğun hashini alma işlemi tekrarlanır. Bu işlem, madenciler arasında ilk çözenin Bitcoin ödülünü kazanacağı bir yarışmadır.
4. Uygun nonce değerini, yani hedef hash değerini ilk bulan madenci bloğu Bitcoin ağında yayınlar.
5. Ağda yayınlanan blok diğer madenci düğümler tarafından kontrol edilerek doğrulanır. Bu doğrulama işlemi bilinen bir verinin hash değerini almak biçiminde çok hızlı ve kolay

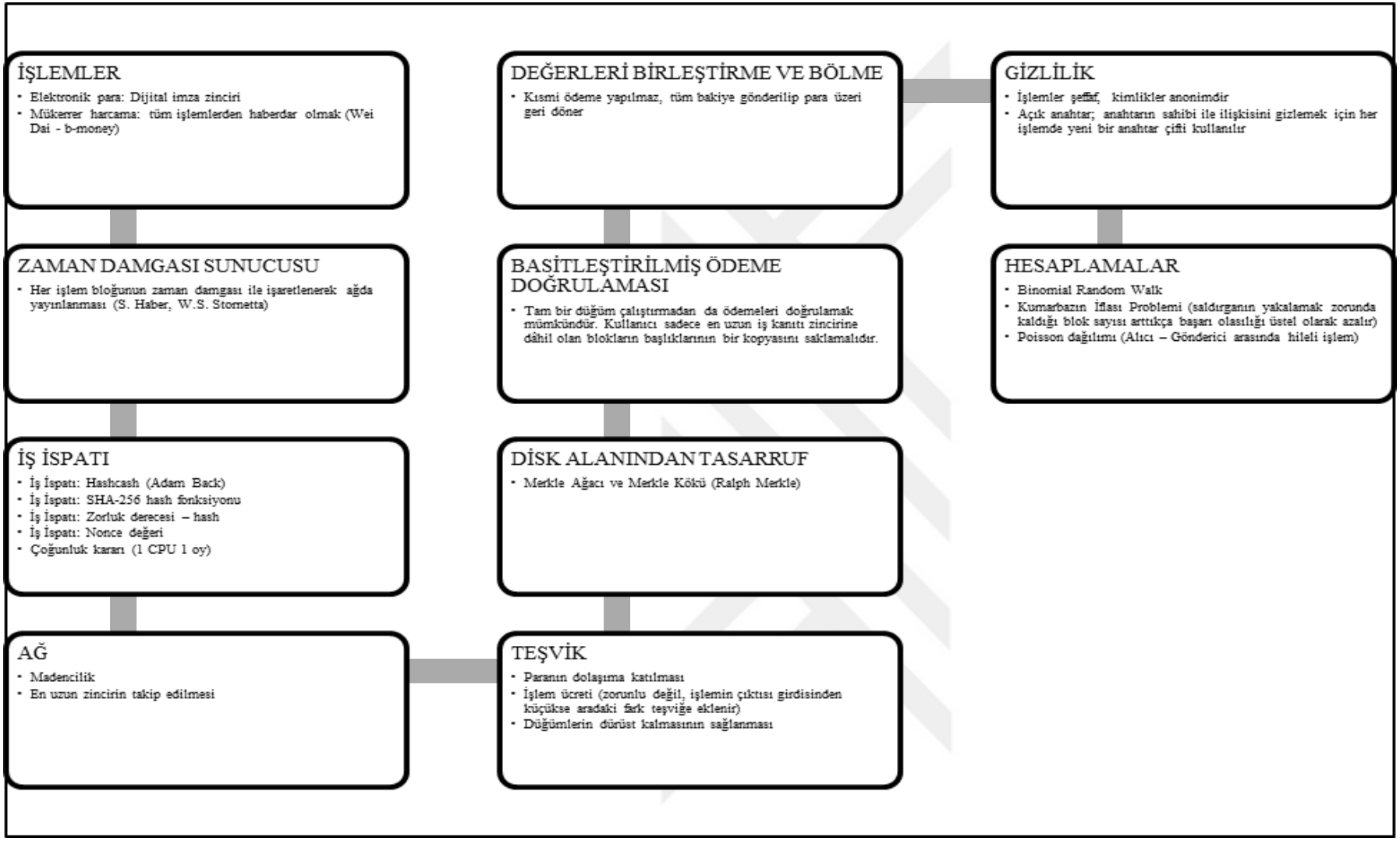
bir işlemdir. Ağdaki düğümlerin yarısından fazlasının onaylaması halinde blok zincire eklenir. Böylelikle bloğun içerisindeki işlemler gerçekleşmiş olur.

6. Ağdaki düğümler eklenen blok doğrultusunda kendi kayıtlarını güncellerler. Yeni işlemlerin ağdaki tüm düğümlere ulaşması zorunlu değildir. Yeterli sayıda düğüme ulaşması yeterlidir. Geçici bir süre ağa bağlı olmayıp daha sonra ağa bağlanan bir düğüm eksik olan blok ya da blokları fark ederek eksik kısmı tamamlamak üzere istekte bulunur. Bu şekilde blok ya da işlem kaybı yaşanmaz.
7. Bu bloğun ilave edilmesi ile en uzun zincir haline gelmiş olan blokzincir esas alınarak bir sonraki blok için aynı işlemler tekrarlanır.



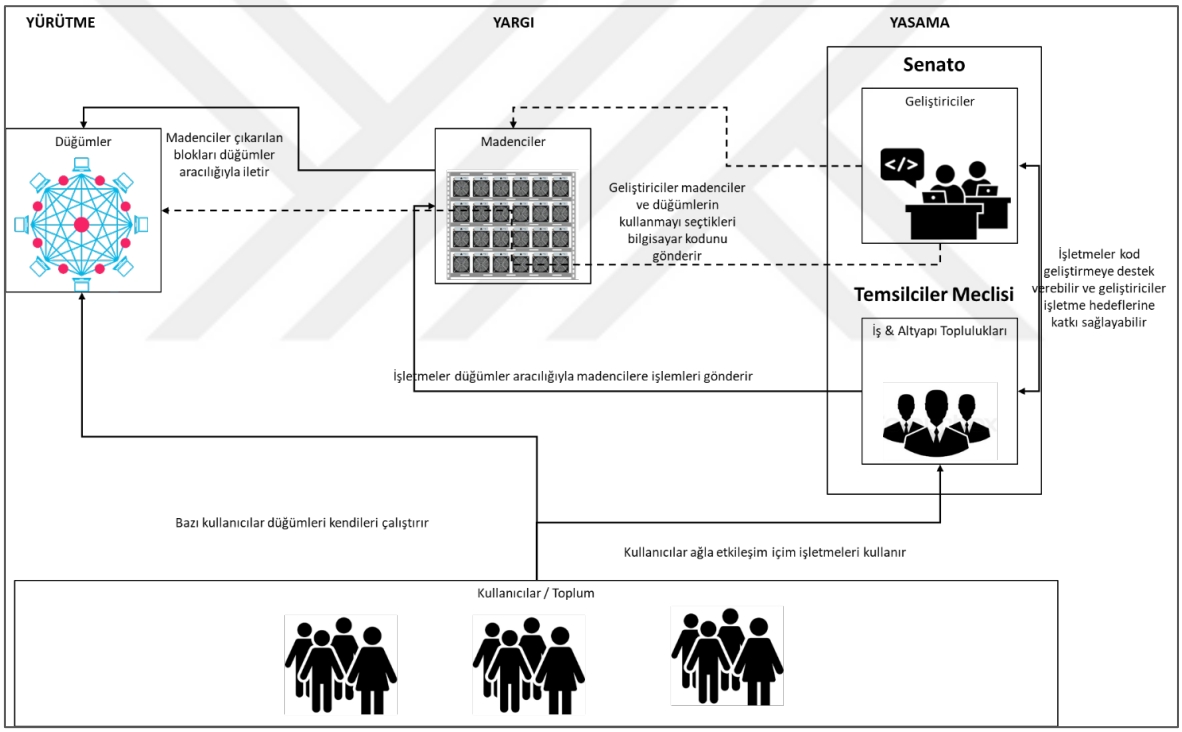
Şekil 2.4. Bitcoin'de blok oluşturma işlem adımları

Nakamoto (2008) Bitcoin'in çalışma prensibini işlemler, zaman damgası sunucusu, iş ispatı, ağ, teşvik, disk alanından tasarruf, basitleştirilmiş ödeme doğrulaması, değerleri birleştirme ve bölme, gizlilik ve hesaplamalar başlıkları altında anlatmıştır. Bitcoin'in tüm özelliklerini içeren bu başlıklar altında sıralanan temel özellikler Şekil 2.5'te verilmiştir. Bu anlatımda, daha önceki bölümde verilenlere ilave olarak teşvik bölümünde düğümlerin dürüst kalmasının, kurallara uymanın sisteme saldırmaktan daha fazla kazandıracağı bir tasarım ile sağlandığı anlatılmaktadır. Tasarıma göre, saldırgan, bütün dürüst düğümlerin toplamından daha fazla işlem gücünü toplamayı başarırsa bu gücü para üretmek için mi yoksa ödemeleri çalarak insanları dolandırmak için mi kullanacağına karar vermelidir. Bu durumda, oyunu kurallarına göre oynamak daha kârlıdır.



Şekil 2.5. Nakamoto (2008) tarafından tarif edilen Bitcoin sistemi ve özellikleri

Bitcoin tasarımındaki kuvvetler ayrılığı ABD hükumet yapısı ile çok paralel bir yapıdadır ve bunun birçok faydası bulunmaktadır. Senatonun yeni tasarılar sunmasına benzer biçimde geliştiriciler yazılım mimarisinde değişiklik ya da güncelleme talepleri sunmaktadır. Yargı sistemine benzer biçimde madenciler geliştiriciler tarafından getirilen kuralları kabul edip etmemeye karar verirler. Yürütme organına benzer biçimde ağdaki düğümler madencilerin çalıştırdığı versiyonu kullanmayarak veto edebilirler. Vatandaşlara benzer biçimde kullanıcılar başkaldırabilir. Son olarak, ekonomik teşvikler sistemde güvenin sürdürülmesi için herkesin en iyiyi yapmasını dikte eder. Örneğin, madenciler kullanıcıları sistemden uzaklaştırdıklarında kripto paranın ya da tokenlerin değeri düşer. Bu biçimdeki Bitcoin yönetişim yapısı Şekil 2.6'da verilmiştir.



Şekil 2.6. Bitcoin yönetişim modelin basit gösterimi (Perley (2017) "A very rough and simplistic diagram of Bitcoin's governance model"den uyarlanmıştır)

2.1.3. Dağıtık kayıt defteri ve blokzincir teknolojisi

Blokzincir teknolojisi ile dağıtık kayıt defteri teknolojisi bazen aynı anlamda kullanılmakla birlikte, blokzincir dağıtık kayıt defteri teknolojisinin bir alt kategorisidir. Dağıtık kayıt defteri teknolojisinde kayıtlar tek bir merkezi yapıda değil dağıtık biçimde tutulur. Blokzincir ise spesifik bir kayıt defteridir. Blokzincirin en önemli farkı tutulan kayıtların

birbirlerine kriptografik metotlarla bağlanmasıdır. Dağıtık kayıt defteri teknolojisi gizli ya da herkese açık olsun kayıtların ve bilginin dağıtılmasını sağlayan teknolojileri tanımlayan şemsiye bir kavramdır. Blokzincir ise ilk tam fonksiyonel dağıtık kayıt defteri teknolojisidir ve çok daha kapsamlı olan bu teknolojinin bir alt kategorisidir. Her blokzincir bir dağıtık kayıt defteridir ancak her dağıtık kayıt defteri bir blokzincir olmayabilir. Her iki kavram da merkezi olmayan bir yapı ve düğümler arasında bir mutabakat işlemi gerektirmektedir.

Dağıtık bir kayıt defteri çok sayıda düğüm veya hesaplama aracı arasında yayılmış olan bir veri tabanıdır. Her düğüm, defterin özdeş bir kopyasını kendisinde muhafaza eder. Ağdaki her düğüm kendisindeki kaydı bağımsız biçimde günceller. Dağıtık kayıt defteri teknolojisinin çığır açan özelliği herhangi bir merkezi otoriteye gereksinim duyulmadan kullanılmasıdır. Defterdeki her güncelleme bağımsız biçimde yapılandırılmıştır ve ağdaki her düğüm tarafından kaydedilir. Daha sonra bu güncellemeler konusunda bir oylama mekanizması ile çoğunluğun onayı alınarak işlemin doğruluğu garanti altına alınır. Bu oylama ve anlaşma mekanizması mutabakat olarak adlandırılır ve bir konsensüs algoritması ile otomatik olarak gerçekleştirilir. Mutabakat sağlandıktan sonra dağıtık kayıt defteri kendisini günceller ve en güncel olan kopya her düğüm noktasında ayrı ayrı kaydedilir. Bu teknoloji, güven maliyetini önemli ölçüde düşürmektedir. Dağıtık kayıt defterlerinin yapısı ve mimarisi bankalar, devletler, noterler ve benzer aracılara olan ihtiyacı azaltır. Bu teknoloji, bilginin nasıl toplandığı ve nakledildiği konusunda yeni bir paradigma sunmakta, bireylerin, kuruluşların ve devletlerin işlemlerini kökten değiştirme potansiyelini taşımaktadır.

Blokzincir teknolojisi dağıtık kayıt defteri teknolojisinin özel bir şeklidir. Blokzincir, yapısı nedeniyle diğer dağıtık kayıt defteri türlerinden ayrılmaktadır. Blokzincirdeki veri bir arada gruplanmış ve bloklar içerisinde düzenlenmiştir. Daha sonra her bir blok birbirine bağlanarak kriptografi kullanımı ile güvenliği sağlanmıştır. Blokzincir temel olarak sürekli büyüyen bir kayıtlar listesidir.

2.1.4. Blokzincirde gizlilik ve mahremiyet

Açık ve izin gerektiren blokzincirlerde, ağdaki düğümler kendi açık anahtarları ile tanımlandıkları için mahremiyet takma adlarla sınırlıdır. İşlemlere ilişkin işlem miktarı, transfer edilen varlık, zaman ve alıcı adresi gibi bilgiler gizli değildir. Blokzincirde gizlilik

verinin yetkisiz üçüncü taraflardan korunması, mahremiyet ise blokzincir kullanıcılarının ve işlemleri gerçekleştiren tarafların kimliklerinin ihlallerden korunması anlamına gelmektedir.

Blokzincirde gizlilik ve mahremiyetin sağlanması için karşılanması gereken koşullar aşağıdaki biçimdedir (Yang, Gavigan ve Wilcox-O'Hearn; 2016):

- Bir işleme dâhil olan tarafların blokzincirde tutulan kimlikleri, meta veriler dâhil olmak üzere, yetkisiz bir üçüncü tarafa ifşa edilmemelidir.
- İşlemde rol alan taraflar bu bilgileri açıklamayı seçmedikleri sürece işlem ayrıntıları yetkisiz taraflarca kullanılamamalıdır.
- İşlem ayrıntıları zincir dışında saklanan bilgilerle harmanlanarak, analiz edilerek veya eşleştirilerek çıkarılamamalıdır. Bu analizler içerisinde kayıt defteri ile ilişkili faaliyetlere dayalı olarak karşı tarafın profilini oluşturmak için grafik analizi, desen eşleştirme ve makine öğrenmesinin kullanımı bulunmaktadır.

Gizlilik ve mahremiyetin artırılması için kullanılan, göndericinin kimliğini, alıcının kimliğini ya da işlem detaylarını gizleyen münferit çözümler bulunmaktadır. Uygulamada, bu teknikleri bir arada kullanarak daha fazla mahremiyet ve gizlilik sağlayan platformlar bulunmaktadır. Örneğin; Zcash sıfır bilgi ispatı (zero-knowledge proof) ve gizli adresleri bir arada kullanmakta, Monero halka yapıları, gizli adresler ve Pedersen taahhütlerini uygulamaktadır.

Blokzincirde okuma erişimini kısıtlamanın en temel yolu blokzinciri özel ve izin gerektiren yapıda tasarlamaktır. Ancak, kullanıcıların işlem detaylarını ağdaki diğerleri ile paylaşmak istememeleri durumunda bu yaklaşım uygun değildir. Okuma erişimini kısıtlamanın alternatif bir yolu işlem detaylarını zincir dışında (off-chain), yani erişim kontrol kısıtlamalarıyla konfigüre edilmiş başka bir sistemde tutmaktır. Bu durumda, blokzincir aktüel işlem detaylarının hash değerini tutar. Bu çözüm birçok uygulamada kullanılmakla birlikte, bilgilerin zincir dışında tutulması halinde blokzincirin artık tek ve paylaşılan bir gerçeklik kaynağı olmayacağı, karşı tarafın kendi kayıtlarını tutması ya da bu sorumluluğu üçüncü bir tarafa devretmesi gerekebileceği unutulmamalıdır.

Yang ve diğerleri (2016) blokzincirde gizlilik ve mahremiyet için kullanılan bazı teknikleri aşağıdaki biçimde sıralamaktadır:

- Tek seferlik adresler: Eğer ağdaki bir düğüm tüm işlemleri gerçekleştirmek için aynı adresi kullanıyorsa bir saldırgan işlemleri gözlemleyerek ilgili tarafların kimlikleri gibi hassas bilgileri elde edebilir. Bu sorunu gidermek için her işlem için tek seferlik bir adres kullanılır. Alıcı taraf işlem gerçekleşmeden önce bir adres oluşturarak gönderene iletir, gönderen de işlemi gerçekleştirirken bu adresi kullanır. Yeni adresin işlem geçmişi olmadığından bir saldırgan tarafından işlem akışının net şekilde gözlemlenmesi ve bir araya getirilmesi zordur. Belirli bir tek seferlik adres alma ve daha sonra gönderme işleminde kullanıldığı için başka adreslerle ilişkilendirilerek ve grafik analiz teknikleri kullanılarak işlemlerin anonimliklerinin ortadan kaldırılmasında kullanılabilir. Tek seferlik adresler karşı taraf sadece belirli bir zaman dilimindeki bir işleme katılımlarını gizli tutmak istedikleri kullanım durumları için uygundur. Bu teknik sadece karşı tarafın kimliğini gizlemeyi hedeflemekte olup işlem detayları blokzincirde yayınlanmaktadır.
- Gizli adresler: Tek seferlik adreslerin kullanımı ve yönetimi zor olabilir. Gizli adresler alıcının değil gönderenin tek seferlik adresler oluşturmasına izin verir. Burada, alıcı tarafından bir ana anahtar çifti oluşturur ve açık anahtarı yayınlar. Gönderen, yeni bir tek seferlik adres oluşturmak için bu adresi kullanır. Alıcı gelecekteki işlem için gerekli olan tek seferlik adresin gizli anahtarını hesaplamak için ana özel anahtarı kullanır.
- Karıştırma: Blokzincirdeki işlemlerin grafik analizlerine karşı kullanılan diğer bir teknik karıştırmadır. Karıştırma temelde birçok düğümden gelen işlem taleplerinin alınıp bunların karıştırılması, uygun alıcılara farklı zamanlarda ve farklı miktarla bölünerek gönderilmesidir. Bu şekilde işlem akışlarının izlenmesi engellenir. Karıştırma işleminin etkili olması için çok sayıda işlem olması ve toplanan işlem taleplerinin gerçekleştirilmeden önce uzunca bir bekleme zamanı geçmesi gerekmektedir. Karıştırma işleminin riskleri ise karıştırma işlemini gerçekleştiren karıştırıcının saldırıya uğraması halinde transfer edilecek tutarların çalınması ve karıştırıcının gönderici ve alıcı bilgilerine sahip olması nedeniyle bu hassas bilgilerin açığa çıkmasıdır.
- Hassas bilgilerin zincir dışında (off-chain) tutulması: Hassas bilgilere erişimin kısıtlanmasının bir diğer yolu bu işlem ayrıntılarının daha sıkı erişim kontrol ksıtlamaları olan başka bir sistemde, zincir dışı olarak saklanmasıdır. Bu durumda, blokzincirdeki işlemler gerçek işlem detaylarının hash değerini içermektedir. Bu hash değerlerinden işlem detayları hakkında bilgi sahibi olmak olanaksızdır. Gerçek işlemlerin detaylarının hash değeri ile blokzincirdeki hash değeri karşılaştırılarak kayıtlar ile işlem detaylarının

uyumu kontrol edilir. Bilgilerin zincir dışında tutulması blokzincirin birçok avantajını ortadan kaldırmakla birlikte güçlü bir gizlilik sağlar.

2.1.5. Blokzincirin potansiyel kullanım alanları ve mevcut uygulamalar

Blokzincir, dijital dönüşümü çeşitli şekillerde kolaylaştırmaya yardımcı olabilme potansiyelini taşımaktadır. Bunlardan en dikkate değer olanlarından biri, tedarik zinciri yönetimi, varlık takibi ve finansal işlemler gibi süreçleri otomatikleştirebilen ve düzene koyabilen akıllı sözleşmelerin kullanılmasıdır. Blokzincirin merkezi olmayan mimarisi, dijital sistemlerde güvenliği ve şeffaflığı artırmaya yardımcı olurken aynı zamanda işlemlerin ve verilerin tahrif edilmesine karşı dayanıklı bir kaydını sağlar. Blokzincir teknolojisinin kullanımı, aracılara ve aracılara olan ihtiyacı azaltarak maliyetleri düşürmeye ve verimliliği artırmaya da yardımcı olabilir. Ek olarak, güvene dayalı olmayan işlemlere olanak tanır ve dijital varlıkların güvenli bir şekilde aktarılmasını sağlar, bu da dijital dönüşüm üzerinde büyük bir etkiye sahip olabilir.

Blokzincirde tutulan veri zaman damgası ile kronolojik olarak sıralandığından, veri yapısı dağıtık, değiştirilemez ve dışarıdan müdahaleye karşı korunaklı olduğundan bilginin kaynağı kolay izlenebilir ve güvenilir hale gelir. Bu temel nitelikler, şeffaflık, izlenebilirlik ve denetlenebilirliğin önemli olduğu alanlardaki uygulamalar için özellikle tercih edilen özelliklerdir.

Uluslararası Telekomünikasyon Birliği Telekomünikasyon Standardizasyon Sektörü (ITU-T) (2019a) dağıtık kayıt defteri teknolojisinin kullanım senaryoları konulu raporunda bu teknolojinin kullanım alanlarını yatay ve dikey olmak üzere iki sınıf altında incelemektedir. Dikey eksende teknolojinin kullanılacağı ana sektörler yer alırken, yatay eksen ise birden fazla sektör için geçerli olan daha genel kullanım alanlarını ifade etmektedir. Buna göre, dağıtık kayıt defteri teknolojisinin dikey kullanım alanları aşağıdaki biçimdedir:

- Finans: En olgun kullanım örneklerinin bulunduğu sektördür. J.P. Morgan tarafından geliştirilen Quorum gibi, bazı bankalar kendi bünyelerinde uygulama geliştirmekte, Goldman Sachs'ın Circle'a yaptığı yatırım gibi bazı bankalar da geliştirme faaliyetlerine finansal destek sağlamaktadır. Finans sektöründe teknolojinin kullanılabileceği alt kategoriler ise aşağıdaki biçimdedir:

  - Kimlik doğrulama (Müşterini Tanı/Kara Paranın Aklanmasının Önlenmesi – KYC/AML)
  - Tokenizasyon ve sabit kripto paralar
  - Finansal yönetim (muhasebe ve denetim)
  - Yolsuzluk riskinin azaltılması
  - Fon sağlama
  - Yatırım araçları
  - Düzenlemelere uyum ve denetim
  - Takas sistemleri
  - Ödemeler ve eşten eşe (P2P) işlemler
  - Yeni ürün modelleri
- Sağlık hizmetleri
  - İlaç endüstrisi (ilaç izleme, şeffaflık)
  - Biyoteknoloji (veri bütünlüğü, mahremiyet ve erişim kontrolleri)
  - Tıbbi kayıtlar (veri gizliliği ve güvenilirliği)
  - Sağlık sisteminde yolsuzlukların önlenmesi
- Bilgi ve iletişim teknolojileri
  - Perakende satış hizmetleri (yeni pazarlar oluşturulması)
  - Toptan satış hizmetleri
  - Nesnelerin interneti
- Sanat, kültür ve e-spor
  - Sanat varlıkları, enstalasyon ve performanslar olarak kripto eserler
  - Telif haklarının korunması
  - İzlenebilirlik ve orijinallik kontrolleri
  - Sanat eserlerinin parçalar halinde sahipliği
  - Sanat eseri sahipleri için sözleşme ve ödeme işlemleri
  - Merkezi olmayan e-spor faaliyetlerinin düzenlenmesi
  - İtibar yönetimi
- Sanayi
  - Tedarik zinciri yönetimi (tarım, uluslararası e-ticaret, madencilik)
  - İklim endüstrisi
- Devlet ve kamu sektörü
  - Mevzuata uygunluk

- Devlet veri yönetimi
- Hukuk
- Vergi
- Vatandaş kimlikleri
- Tapu – mülk kayıtları

Dağıtık kayıt defteri teknolojisinin yatay kullanım alanları ise aşağıdaki biçimdedir:

- Kimlik yönetimi (güvenlik, mahremiyet ve taşınabilirlik – tıbbi kayıtlar, banka müşterileri kredi değerlendirmeleri, hassas alanlara erişim yönetimi)
- Güvenlik yönetimi (kuruluş varlıklarının tanımlanması, bu varlıkların korunması için politika ve prosedürlerin geliştirilmesi, belgelendirilmesi ve uygulanması konularında gizlilik, bütünlük ve kullanılabilirliğin (CIA) sağlanması)
- Veri yönetimi (veri kaynağının izlenebilmesi, şifreleme ve özel anahtarlarla güvenlik)
- Yönetişim ve Merkezi Olmayan Otonom Organizasyonlar (DAO)
  - Ayrı bir varlık olarak kendi kimliği olan, insanlar tarafından değil bilgisayar kodları ile kendi kendini yöneten, halka arz edilerek token sahiplerine eşit haklar veren, idari faaliyetleri azaltarak şeffaflığı artıran kuruluşlar
- Kripto altyapı
  - CoinMarketCap'ın (2022) verilerine göre 26 Ekim 2022 tarihi itibariyle çıkarılan ve ticareti yapılan kripto varlıkların sayısı 21 514'e, kripto para borsalarının sayısı ise 520'ye ulaşmış, kripto varlıkların piyasa değeri ise 991,7 milyar $'ı aşmıştır. Bu piyasanın arkasında kripto para borsaları, uygulama geliştiriciler, madenciler, cüzdan sağlayıcılar, blok üreticileri, madencilik havuzları, düğümler ve kullanıcılar gibi büyük bir ekosistem bulunmaktadır.

Blokzincir teknolojisinin kamu sektöründeki kullanım alanı olarak kimlik yönetimi, tapu kayıtları ve elektronik oylama öne çıkmaktadır (Killmeyer, White ve Chew, 2017). Berryhill, Bourgery ve Hanson'a (2018) göre blokzincir konusundaki gelişmeler daha çok finans alanında yaşanmakta olup kamu sektöründeki uygulamalarda en sık karşılaşılan konular sağlık ve mali bilgileri içeren kişisel kayıtların tutulması, dijital kimlikler, sosyal yardımların izlenmesi, tapu kayıtları ve tedarik zinciridir. Berryhill ve diğerleri (2018) blokzincir teknolojisinin kullanılmasının avantaj sağlayacağı alanları; kimlik yönetimi

(yeterlililik belgeleri, lisanslar vb.), kişisel kayıtların yönetimi (sağlık, sigorta, mali vb.), finansal hizmetler ve bankacılık, tapu kayıtları, tedarik zinciri yönetimi, varlık takibi ve envanter izleme, sosyal yardımlar, hak sahiplikleri, sözleşme ve tedarikçi yönetimi, telif hakları, enerji tesisleri, oy verme, yolsuzlukların tespiti ve azaltılması, kuruluşlar ve sektörler arası süreçlerin düzenlenmesi biçiminde sıralamaktadır. Ayrıca, doğum kayıtları, evlilik cüzdanları, pasaport ve vize bilgileri, ölüm kayıtları gibi birçok farklı kimlik özelliğinin yönetiminde blokzincir teknolojisinin kullanılabileceğini ileri sürerek yürütülmekte olan blokzincir proje konuları arasında kimlik yönetiminin sayı bakımından ikinci sırada olduğunu belirtmektedir.

Wüst ve Gervais (2018) blokzincir teknolojisinin tedarik zinciri yönetimi, bankalararası ve uluslararası ödemeler, akıllı sözleşmeler, merkezi olmayan otonom kuruluşlar, fikri mülkiyet hakkı sahipliğinin kanıtlanması, elektronik oylama, nesnelerin interneti, tapu kaydı, ticaret ve adil alışveriş platformları gibi alanlarda kullanım için uygun olduğunu ileri sürmektedir. Halihazırda bu konulara ilişkin gerçek dünya uygulamaları geliştirmiş olan kuruluşlar bulunmaktadır. Tedarik zinciri yönetimi konusunda Skuchain, Provenance, Everledger, küresel çapta bankalararası ödeme konusunda Ripple bu kuruluşlara örnek olarak verilebilir.

Walport (2016) blokzincir teknolojisinin vergi toplama, sosyal yardımların dağıtılması, tapu kayıtlarının tutulması, pasaport işlemleri, tedarik zinciri yönetimi gibi devlet hizmetlerinde kullanılabileceğini belirterek bu teknolojinin devlet hizmetlerinin ve farklı kurumlarda tutulan kayıtların bütünleştirilmesine yardımcı olacağını öne sürmektedir.

Avrupa Parlamentosuna sunulmak üzere 2017 yılında hazırlanmış olan “Blokzincir teknolojisi hayatımızı nasıl değiştirecek?” başlıklı raporda blokzincirin kullanım potansiyelinin en yüksek olduğu konular dijital paralar, dijital içerik ve telif hakları yönetimi, patent, elektronik oylama, akıllı sözleşmeler, tedarik zinciri yönetimi ve merkezi olmayan otonom kuruluşlar olarak belirtilmiştir (Boucher, Nascimento ve Kritikos, 2017).

Maupin (2018) bu teknolojinin tüm dünya vatandaşlarını kapsayan küresel bir dijital ekonominin inşa edilmesi için çok önemli bir fırsat olduğunu belirterek bokzincirin ekonomik direncin geliştirilmesi, finansal kapsamın geliştirilmesi, vergilendirme, ticaret ve

yatırım, istihdam, iklim, sağlık, sürdürülebilir gelişim ve kadının güçlendirilmesi gibi alanlara odaklanan politik amaçlar doğrultusunda kullanılmasını önermektedir.

Lüksemburg Ekonomi Bakanlığı'nın desteği ile Lüksemburg Standardizasyon, Akreditasyon ve Ürün ve Hizmet Kalitesi Enstitüsü (ILNAS) ve Standardizasyon ve Bilgi Ekonomisi Ajansı (ANEC) (2018) tarafından hazırlanmış olan Blokzincir ve Dağıtık Kayıt Defteri Teknolojileri konulu raporda blokzincirin temel özellikleri tokenler/kripto paralar, güvenli veri kaydı ve akıllı sözleşmeler olarak üç ana sınıfa ayrılmış, her bir sınıf için muhtemel kullanım alanları da ödemeler ve havaleler, sermaye bulma, bankacılık ve finansal hizmetler, tapu kayıtları, kimlik yönetimi, eğitim sertifikaları, sağlık kayıtları, tarım ve gıda, imalat, tedarik zinciri yönetimi, enerji alışverişi, perakende, akıllı şehirler ve sanat piyasası olarak sıralanmıştır.

Miller ve Mockel (2019) blokzincir teknolojisinin iklim değişikliği ile mücadele ve sera gazları emisyonunun azaltılması çalışmalarına yardımcı olacak uygulamalarda kullanılabileceğini ileri sürmektedir. Blokzincir teknolojisinin akıllı sözleşmeler ve nesnelerin interneti ile birlikte kullanımı ile enerji alanında; yenilenebilir enerji piyasalarında sertifikasyon ve enerji kaynağının izinin sürülmesi, yenilenebilir enerji üreticilerinin ürettikleri enerjilerin akıllı sözleşmeler aracılığı ile dağıtımı ve pazarlanması, elektrikli araçların nesnelerin interneti ve akıllı sözleşmeler kullanılarak oluşturulacak dolum istasyonları ağını kullanarak şarj edilmesi gibi uygulamalar geliştirilmektedir.

Davradakis ve Santos (2019) blokzincir teknolojisinin potansiyel kullanım alanlarını akıllı sözleşmeler, paylaşım ekonomisi, kitlesel fonlama, yönetişim, tedarik zinciri denetimi, dosya depolama, fikri mülkiyet haklarının korunması, nesnelerin interneti, kimlik yönetimi, kara paranın aklanmasının önlenmesi ve müşterini tanı yükümlülükleri, veri yönetimi, mülkiyet kaydı, hisse senedi ticareti olarak sıralamaktadır.

Hileman ve Rauchs (2017) kamu sektöründe blokzincir teknolojisinin kullanım alanlarını merkez bankaları ve diğer kuruluşlar olarak iki grupta incelemiş, merkez bankalarının bu teknolojiyi bankalar arası ödemeler, havaleler, gerçek zamanlı brüt hesap kapatma sistemi, varlık devri, menkul kıymet takas sistemleri, finansal mesajlaşma sistemi, sendikasyon kredileri ve ticari finansman olarak sıralamaktadır. Diğer kamu kurumlarının ağırlıklı olarak üzerinde çalışmakta oldukları başlıca alanlar ise kimlik yönetimi, mülkiyet kayıtları

yönetimi, kişisel kayıtların saklanması, tedarik zinciri yönetimi, gıda ürünlerinin takibi, araç filolarının izlenmesi, oylama, ödemeler, vergi toplama, nesnelerin interneti, sadakat puanı ve ödülleri, kitlesel fonlama olarak listelenmektedir.

Dünya Bankası (2019: 1) tarafından yayınlanmış olan Gelişim için Kimliklendirme (ID4D) Kılavuzuna göre dünya üzerinde 2018 yılı itibariyle kimliği bulunmayan yaklaşık bir milyar insan bulunmaktadır. Birleşmiş Milletler de mülteciler, insan ticareti mağduru çocuklar, evsizler ve toplum dışına itilmiş bazı kişilerin kurumsal bir bağları olmadan yaşadıklarını doğrulamaktadır. Blokzincir teknolojisinin kullanımının kayıt dışında kalan bu insanlarla ilgili bazı fırsatlar yaratacağı düşünülmektedir.
Sosyal yardımlar için blokzincir teknolojisinin kullanılması banka masraflarından tasarruf etmenin yanı sıra yardımların doğru yere ulaştığından ve doğru biçimde kullanıldığından emin olunmasını da sağlar.

Uluslararası Çalışma Örgütü (ILO) en az 21 milyon insanın insan kaçakçılığından etkilendiğini, bunların da %26'sından fazlasının çocuk olduğunu tahmin etmektedir. Blokzincir teknolojisine dayalı kimliklerin bu soruna çözüm olabileceği düşünülmektedir. Bu sorunla ilgili çarpıcı bir örnek çocuk kaçakçılığının yoğun biçimde yaşandığı, Avrupa'nın en yoksul ülkelerinden biri olan Moldova'dır (Lubin, Anderson ve Thomason, 2018). Moldova hükumeti Birleşmiş Milletler uzmanları ile birlikte, bu konu ile ilgili olarak, blokzincire dayalı dijital bir çözüm üzerinde çalışmaktadır. Özellikle kırsal kesimde yaşayan çocuklar risk altında olup buralarda yaşayanların resmi olarak kimlik kayıtlarının bulunmaması onları kolay hedef haline getirmekte, sahte belgelerle sınır dışına çıkarılmalarını kolaylaştırmaktadır. Blokzincir ile kâğıt ortamında olmayan, parmak izi veya yüz tarama gibi biyometrik verilerle oluşturulmuş dijital kimlikler bu sahte belgelerle sınırı geçme olayını imkânsız hale getirecektir.

Lubin ve diğerleri (2018) blokzincir teknolojisinin 2011 yılından bu yana Suriye'den ayrılarak ağırlıklı olarak Türkiye, Lübnan ve Ürdün'de yaşamak zorunda kalan okul çağındaki 1,6 milyondan fazla çocuğun eğitimlerinin desteklenmesi için yapılan 1,4 milyar $ yardımın daha iyi koordine edilmesi ve raporlanması için kullanılabileceğini ileri sürmektedir.

Niforos (2017) blokzincir teknolojisinin finans kuruluşları tarafından kurumlar arası projelerde, karmaşıklığı ve maliyetleri azaltarak etkinliği artırmak amacıyla kullanılmasının çok daha muhtemel olduğunu öne sürmektedir. Blokzincirin potansiyel etkileri ve kullanım alanları mevcut faaliyetlerin etkinliğinin artırılması ve yeni pazarlar yaratılması olmak üzere iki ana başlık altında toplanabilir. Halihazırda birçok banka blokzincir şirketleriyle birlikte blokzincir teknolojisinin mevcut süreçlerinde kullanımı üzerinde çalışmaktadır. Örneğin, R3 konsorsiyumu 70 global bankanın dâhil olduğu bir dağıtık kayıt defteri sistemi ile Corda adlı protokolü kullanarak bir mesajlaşma ağı oluşturmuştur. Dünya çapında 75 bankanın dâhil olduğu Ripple ise bokzincir teknolojisini kullanarak uluslararası ödemeleri çok daha hızlı ve düşük maliyetli biçimde gerçekleştirmektedir. Blokzincir teknolojisinin ortaya çıkardığı yeni pazar fırsatlarına örnek olarak fiyat paraya alternatif bir ödeme sistemi ve finansal sisteme dahil olmayan insanlar için sunduğu dijital kimlik çözümleri sayılabilir. Finansal sisteme erişimi olmayan yaklaşık bir milyar insanın blokzincir teknolojisi ile yaratılan yeni bir sisteme katılımının sağlanması ve işlem komisyonları %5 ile %30 arasında değişen, 4 milyar $'lık küresel havale pazarındaki komisyon oranlarını önemli oranda azaltma potansiyeli finansal açıdan sağlayacağı yıkıcı etkiler olarak değerlendirilmektedir. Blokzincire dayalı kimlik sistemi, kullanıcıların kendi verilerine tam hakim olmalarını ve kendi verilerinin istedikleri kısmını, istedikleri kişi ya da kurumlarla paylaşabilmelerine izin vermektedir. Örneğin, ABD merkezli UPort Ethereum altyapısını kullanan dijital kimlik yönetimi çözümü ile hem son kullanıcılar hem de kuruluşlar için kendi kendine egemen kimlikler sunmaktadır. Cambridge Blockchain LLC, Gem, Londra merkezli CreditsVision, Singapur merkezli KYCK, Hindistan merkezli Elemential gibi firmalar dijital kimlik çözümleri geliştirmektedir.

Ledger Insights (2020) Pekin belediyesince yürütülmekte olan, blokzincir teknolojisinin kullanıldığı 140 kamu uygulamasının üç temel kategoriye ayrılmış olduğunu belirtmektedir: veri paylaşımı ve alışverişi, kuruluşlar arası işbirliği süreçleri, elektronik sertifikaların yönetimi ve saklanması. Aktarılan raporda yer alan bazı spesifik kullanım alanları uluslararası lojistik ve taşıma, müşterini tanı ve kimlik doğrulama, elektronik fatura, KOBİ finansal hizmet platformu, tedarik zinciri yönetimi, gayrimenkul kayıt sistemi, kimlik, sürücü belgesi ve evlilik cüzdanlarının kaydıdır.

Devletin en önemli fonksiyonlarından biri bireyler, kurumlar, varlıklar ve faaliyetler hakkında bilginin güvenilirliğini sağlamaktır. Farklı devlet kurumları doğum ve ölüm

kayıtları, medeni durum, ehliyet, mülk alım-satımı veya adli faaliyetler ile kayıtları tutmak ve sürdürmekle görevlendirilmişlerdir. Çok gelişmiş devletler için bile bazen bu kayıtları yönetmek ve kullanmak çok karmaşık olabilmektedir. Bazı kayıtlar sadece kâğıt ortamındadır ve resmi kayıtlarda bir değişiklik yapılması gerektiğinde vatandaşın birebir başvuruda bulunarak kendisini göstermesi gerekmektedir. Her kuruluş kendi görev sahasına giren konularda kendi veri depolarını ve bilgi yönetim protokollerini oluşturmakta, devletin diğer organlarının bunları kullanmasına izin vermemektedir. Bazı durumlarda da farklı kurumlar benzer ya da aynı verileri farklı biçimlerde tutmakta, bu da bazen çelişkili verilerin ortaya çıkmasına ve verimsizliğe neden olmaktadır. Verilerin yetkisiz erişime veya manipülasyonlara karşı korunması ise bir başka sorumluluk, risk ve maliyet alanıdır. Blokzincir teknolojisi güvenilir bilginin yönetimini kolaylaştırmakta, devlet kuruluşlarının kritik kamu sektörü verilerine erişimini, bu verilerin kullanımını ve bu bilgilerin güvenliğinin sağlanmasını kolaylaştırmaktadır.

Blokzincir teknolojisinin kullanım örneklerinden biri de alıcı ve satıcıları bir araya getiren çevrimiçi alışveriş platformlarıdır. OpenBazaar tamamen merkeziyetsiz çevrimiçi bir pazaryeridir. Platformda 50'den fazla kripto para kullanarak alımsatım işlemleri gerçekleştirebilmektedir.

Blokzincir gıdanın menşei ve durumu ile ilgili doğrulanmış bilgileri kaydederek izlenebilirliği artırmak ve gıda sahtekarlığını azaltmak için kullanılabilmektedir. Bir yandan, değer zincirindeki tüm taraflar (çiftçiler, tedarikçiler, işleyiciler, distribütörler, perakendeciler, tüketiciler ve düzenleyiciler) gıda ürünü hakkında gerçek zamanlı bilgilere erişebilirken (örneğin, kontamine olmuş ürünleri kaynağına kadar izlemek, gıdanın çocuk işçiliği olmadan üretildiğini doğrulamak) diğer taraftan kullanıcılar çiftlikten perakendeciye kadar tüm ürün yaşam döngüsünü geriye doğru izleyebilmektedir. Walmart tarafından blokzincir teknolojisi kullanılarak yapılan testte, daha önce 6 gün alan mangoların izini sürme çalışması 2,2 saniyede tamamlanmıştır (ILNAS ve ANEC, 2018).

Birleşmiş Milletler Gıda ve Tarım Örgütü (FAO), yenilikçi gıda sistemleri oluşturmak ve gıda güvenliğini, emniyetini ve pazar verimliliğini artırmak için hayati bir e-tarım altyapısı bileşeni olarak blokzincir teknolojisinin kullanılmasını önermektedir (Lin ve diğerleri, 2017).

Blokzincir, karmaşık tedarik zincirlerinde ürünün kökeninin kaydı, akıllı sözleşmelerle anlaşmaların uygulanmasının otomatikleştirilmesi ve diğer farklı güçlüklerin üstesinden gelinmesi için yeni bir yöntem sunmaktadır. Tedarik zincirlerinde blokzincirin kullanımı dev perakendecilerden nakliye limanlarına, çelikten elmas ve sanat eseri gibi değerli emtialara kadar küresel bir ilgi görmüştür. Bu girişimlere örnek olarak gıda güvenliği ve izlenebilirliğini geliştirmek için Walmart, IBM, Çin perakende firması JD.com ve Tsinghua Üniversitesi tarafından kurulan Blokzincir Gıda Güvenliği Birliği, Danimarkalı nakliye firması Maersk tarafından Microsoft, Willis Tower Watson ve sigorta firmaları ile birlikte geliştirilen denizclik sigortasının takibi uygulaması, nakliye maliyetlerinin azaltılması, mevcut tedarik zinciri sürecindeki verimsizliklerin giderilmesi amacıyla Maersk ve IBM tarafından geliştirilen küresel ticaret platformu, Rotterdam Limanı tarafından kurulan BlockLab, sanat eserlerinin izlenmesi için Deloitte Lüksemburg tarafından geliştirilmiş olan ArtTractive verilebilir.

Kişisel verilerin korunması blokzincir teknolojisinin avantaj sağlayacağı alanlardan biridir. Kuruluşların veriyi korumak için gösterdikleri büyük çabaya karşın kamu hizmetlerinden faydalananlar, verilerine illegal erişim sağlanmasından endişe duymaktadırlar. Şifreleme metotları %100 güvenlik sağlayamaz ancak blokzincir teknolojisi benzer ihlallerin gerçekleşmesini çok güçleştiren bir teknolojidir. Örneğin, Estonya, Şifresiz İmza Altyapısı (KSI) adı verilen bir teknoloji kullanarak tüm kamu sektörü verisini korumaktadır.

Varlıkların sahipliği ve el değiştirmesi birçok farklı tarafın etkileşimini ve resmi belge işlemini gerektirmektedir. Blokzincir teknolojisiyle bu işlemler çok daha kolay ve pratik hale getirilebilmektedir. Malvarlığının blokzincir ile izlenmesinin bir diğer faydası ise veriye ilişkin tüm hareketlerinin izlenebilmesi sayesinde bu varlıklara yetkisiz biçimde erişilmesinin ve verilerde manipülasyon yoluyla yolsuzluk yapılmasının önüne geçilmesidir.

Allessie, Sobolewski ve Vaccari (2019) blokzincir teknolojisinin kamu hizmetlerinde kullanımına ilişkin olarak yaptıkları çalışmada tespit ettikleri spesifik bulguları aşağıdaki biçimde listelemiştir:

- Noter onayı, paylaşılan veri tabanı ve iş akışı otomasyonunun vatandaşlar ile işletmelerin etkileşimleri için faydalı ve kamu hizmetlerinin operasyonel kapasitelerinin geliştirilmesi için faydalı olacağı değerlendirilmektedir.

- Blokzincir teknolojisine dayalı noter işlemlerine ilişkin kullanım örnekleri daha olgun olmakla birlikte, daha yıkıcı nitelikteki kullanımlarda mevcut süreçlerle ve yasal düzenlemelerle uyumsuzluk nedeniyle bazı uygulama zorluklarıyla karşı karşıya kalınmaktadır.
- Olgunluk düzeyi daha yüksek olan projelerin daha merkezi bir yönetim yapısına ve daha az sayıda paydaşa sahip olma eğiliminde oldukları gözlenmektedir.
- Hâlihazırda kullanımda olan blokzincire dayalı hizmetlerin kuruluşların net gereksinimlerine karşılık verdikleri görülmektedir. Bu hizmetlerde aynı zamanda aktif bir kamu sektörü aktörü ve güçlü bir teknolojik ortak yer almaktadır.
- Blokzincir uygulamaları büyük oranda açık kaynak kodlu yazılımlara dayanmaktadır. Bazı devletler üçüncü tarafları daha fazla teşvik etmek ve tek kaynağa bağımlılık riskini en aza indirmek için platformdan bağımsız açık kaynak kod standartlarının yayınlanması için uğraşmaktadır.
- Blokzincir, daha gelişmiş bir hizmetin sadece bir katmanıdır. Blokzincir çözümü genellikle geleneksel, merkezi bir veri tabanının üzerinde çalışan dağıtık kayıt defteri teknolojisi olmayan bir katmana bağlıdır.
- Gizli veriler daima zincir dışında (off-chain) tutulur. Özel ve izin gerektiren bir blokzincir kullanıldığında veri prensip olarak zincir içerisinde, şifrelenmiş olarak tutulabilir. Bununla birlikte, veri, zincir üzerinde tutulduğunda, ağ üzerinde transfer edilen verinin boyutu sürekli olarak arttığından bu durum bazı verimsizliklere neden olmaktadır ve bu nedenle bu tasarım pek pratik değildir.
- İşlem hacmi çok önemli bir darboğaz olarak görünmemektedir. İzin gerektirmeyen blokzincir protokollerinde işlem hacmi, okuma, yazma ve işlem doğrulama için izin gerektiren protokollere göre çok daha düşüktür. Bu nedenle, açık ve izin gerektirmeyen blokzincirlere bağlı projelerde işlem hacmi kısıtlarını giderecek bir tasarım yapılmalıdır.
- Blokzincir teknolojisi hâlihazırda kamu kuruluşlarının aracılık rolleri için bir tehdit oluşturmamaktadır. Blokzincire dayalı çözümler daha çok tamamlayıcı veya mevcut çevrimiçi hizmetlerin yerini sadece kısmen alacak yapıdadır.
- Analiz edilen blokzincir tasarımları belirli maliyet kalemleri doğurmaktadır ancak bunların toplam maliyetleri merkezi tasarımların uygulama maliyetlerinden yüksek olmamalıdır.
- Blokzincire dayalı hizmetlerin kamu sektörü için sağlayacağı temel fayda kayıt saklama konusundaki etkinliği ve güvenilirliği artırarak kamu kuruluşlarına olan güveni

artırmasıdır. Ayrıca, kamu kuruluşları ile etkileşimde olan vatandaşlar ve işletmelerin işlerini de kolaylaştıracaktır.

Yapılan literatür araştırmasının sonuçları, dünyadan kullanım örnekleri ve yürütülmekte olan projeler değerlendirildiğinde blokzincir teknolojisinin kullanım alanının sürekli genişlemekte olduğu ve kullanım sahası bakımından bazı konuların blokzincir teknolojisinin yapısal özelliklerine uygunlukları nedeniyle öne çıktığı görülmektedir. Teknolojinin kullanımının en fazla rastlandığı konular bu bağlamda Çizelge 2.3'te verildiği biçimde listelenmiştir.

Çizelge 2.3. Blokzincir teknolojisinin başlıca kullanım alanları

Kullanım Alanı	Sektör
Nesnelerin interneti	Bilgi ve İletişim Teknolojileri
Mesajlaşma sistemi	Bilgi ve İletişim Teknolojileri
Yenilenebilir enerji (sertifikasyon, enerji kaynağının izlenmesi, enerji satışı)	Enerji
Müşterini Tanı (KYC)	Finans
Kara Paranın Aklanmasının ve Terörün Finansmanının Önlenmesi (AML)	Finans
Tokenizasyon ve sabit kripto paralar	Finans
Fon toplama, finansman ve kredi sağlama (Kitlesel fonlama - İlk Dijital Para Arzı ICO)	Finans
Takas sistemleri	Finans
Ödemeler, havaleler ve eşten eşe işlemler	Finans
Sanat eseri sahipleri için sözleşme ve ödeme işlemleri	Finans
Dijital paralar	Finans
Bankalararası ve uluslararası ödemeler	Finans
Mikro ödemeler	Finans
Sadakat puanı ve ödemeleri	Finans
Mevzuat sistemi	Kamu hizmetleri
Devlet veri yönetimi	Kamu hizmetleri
Hukuk	Kamu hizmetleri
Vergi toplama	Kamu hizmetleri
Gayrimenkul kayıtları	Kamu hizmetleri
Sosyal yardımların dağıtılması ve takibi	Kamu hizmetleri
Telif haklarının korunması	Patent ve hak sahipliği
İzlenebilirlik ve orijinallik kontrolleri	Patent ve hak sahipliği
İlaç endüstrisi (ilaç izleme)	Sağlık
Tıbbi kayıtların tutulması	Sağlık
Tedarik Zinciri Yönetimi	Sanayi ve ticaret
Kişisel verilerin korunması	Siber güvenlik
Gıda ürünlerinin izlenmesi	Tarım ve gıda

Dijital kimlikler ve kimlik yönetimi (kimlik, sürücü belgesi, evlilik cüzdanı, sertifika, diploma, yeterlilik belgeleri, lisanslar vb.)	Veri yönetimi
Veri güvenliği	Veri yönetimi
Varlık takibi ve envanter izleme	Veri yönetimi
Sanat varlıkları, enstalasyon ve performanslar olarak kripto eserler	Yeni pazarlar
Sanat eserlerinin parçalar halinde sahipliği	Yeni pazarlar
Çevrimiçi alışveriş	Yeni pazarlar
Akıllı sözleşmeler	Yönetim ve yönetişim
Kuruluşlar arasında bilgi paylaşımı	Yönetim ve yönetişim
Elektronik oylama	Yönetim ve yönetişim

Sonuç olarak, blokzincir, dijital dönüşümü kolaylaştırmak için birçok kamu hizmetinde kullanılabilecek bir teknolojidir. Finansal işlemlerin yürütülmesi, dijital varlıkların yönetimi ve hizmetlerin sağlanması gibi çok çeşitli süreçleri otomatikleştirebilen akıllı sözleşmelerin otomasyonun sağlanmasında kullanılması dijital dönüşümün hızlandırılması için bir fırsat olarak değerlendirilmektedir.

2.1.6. Blokzincirin güçlü yönleri ve sunduğu fırsatlar

OECD tarafından yayınlanan Kamu Yönetimi Üzerine Çalışma Raporlarından 28 inci sıradaki Blokzincir Teknolojisi ve Kamu Sektöründe Kullanımı başlıklı olanına göre blokzincir teknolojisinin en önemli özelliklerinden biri dağıtık ve paylaşılan yapısıdır. Bu özelliği ile blokzincir, mevcut aracıların sebep olduğu maliyetleri ve ihtilafları ortadan kaldırarak aracıya gerek duyulmayan dağıtık bir güven ortamı ve düşük işlem maliyetleri ile daha fazla veri bütünlüğü vadetmektedir. Ayrıca, hizmetlerin sürekliliği konusundaki tek nokta hatasını ortadan kaldırma, yolsuzluk ve hataların azaltılması, kâğıt yoğun süreçlerin maliyetinin düşürülmesi, devlet tarafından tutulan veriler ve yürütülen işlemler üzerinde şeffaflık sağlanması konularında yardımcı olma potansiyelini taşımaktadır (Berryhill ve diğerleri, 2018: 7, 11).

ITU-T dağıtık kayıt defteri teknolojisi kullanım senaryoları konulu teknik raporunda (2019a) teknolojinin genel faydaları arasında güvenli, maliyet etkin, sistemik hatalara ve dışardan müdahaleye dayanlıklı, denetlenebilir, yolsuzlukları tespit edebilir ve azaltabilir bir teknoloji olması sayılmaktadır. Aynı raporda, bu teknolojinin diğer sektörlere ve teknolojilere de kazanç sağlama imkanı verecek genel amaçlı bir teknoloji olduğu vurgulanmaktadır. Genel amaçlı diğer teknolojiler olarak sıralanan buhar enerjisi, elektrik

ve internet gibi dağıtık kayıt teknolojileri de güven, anonimlik, veri saklama ve işleme yöntemi bakımlarından veriye bakışta bir devrim meydana getirmiştir. Teknolojinin diğer avantajları ise aşağıdaki biçimde listelenmektedir:

- Şeffaflık ve güven
- Güvenlik
  - Veri şifreleme
  - Erişim kontrolleri
  - Silmeye ve değiştirmeye karşı korunaklı veri
  - Kimlik yönetimi
  - Hata toleransı
- Ekonomik ve sosyal teşvikler
  - Aracıların ortadan kaldırılmasıyla düşen maliyetler
  - Yeni gelir alanları
  - Hızlı ve her an gerçekleştirilebilir işlemler
  - Finansman sağlama kolaylıkları
- Etkinliğin artırılması ve karmaşıklığın azaltılması
  - Aracıların fazla olduğu süreçleri sadeleştirme
  - Manuel işlemleri azaltma, doğrulama ve denetim faaliyetlerini kolaylaştırma

Japonya Ekonomi, Ticaret ve Sanayii Bakanlığı'na bağlı Nomura Araştırma Enstitüsü (2016) tarafından hazırlanmış olan rapora göre geleneksel merkezi sistemlerle karşılaştırıldığında blokzincir teknolojisinin temel yapısal özeliklerinin öne çıktığı konular, arıza süresi sıfır olan bir sistem sunması, sahtecilik ve tahrifat yapılmasının hemen hemen imkânsız olması ve mevcut sistemlere göre hizmetleri çok daha düşük maliyetlerle karşılama potansiyelini taşımasıdır.

Blokzincir teknolojisinin ortaya çıkış sürecinde, Bitcoin'in duyurularak kullanılmaya başlanması ile başarılabileceği ispatlanan temel motivasyon ve arka plandaki felsefe bireylere mahremiyet, muktedirlere ise şeffaflık sağlayan, merkezi otoriteler ile teknoloji devlerine olan bağımlılığı ortadan kaldıran bir mekanizmanın kurulmasıdır. Bu mekanizmanın kurulması için uzun yıllar boyunca tamamen kriptoloji, matematik ve yazılıma dayalı çözümler üzerinde çalışılmış, tüm bu çalışmaların bir ürünü olarak da ilk olarak Bitcoin ile bu felsefenin hedeflerine ulaşılabileceği ispatlanmıştır.

Teknik altyapısı ve mimarisinden kaynaklanan şeffaflık, gizlilik, güvenlik ve dağıtık yapısı ile blokzincirin gündelik hayatta kullanımının getireceği bazı avantajlar aşağıdaki biçimde listelenmektedir:

- Doğrulama ve güvence verme fonksiyonunu taşıyan aracılara gerek duyulmaması nedeniyle işlem maliyetlerinde azalma,
- Mikro ve nano ödemeler olarak adlandırılan çok küçük miktarlı transfer işlemlerinin gerçekleştirilebilmesi,
- Bankacılık sistemine dâhil olmayan insanların finans işlemleri gerçekleştirebilmelerine olanak sağlanması,
- Kişilerin kendi verilerinin sahibi olarak bu verilerin yönetiminde tam yetki sahibi olmaları,
- Kişisel mahremiyet ihlal edilmeden farklı taraflar arasında veri paylaşımının mümkün olması,
- Veri koruma maliyetinin düşürülmesi,
- Kaynak toplamayı kolaylaştırması.

Avustralya ve Yeni Zelanda Yetkili Muhasebeciler Birliği tarafından yayınlanmış olan Blokzincirin Geleceği: Dağıtık Kayıt Defteri Teknolojisinin Uygulamaları ve Etkileri başlıklı raporda (2017) blokzincir teknolojisinin ihtilafların giderilmesi ve farklı birimler arasındaki mutabakat işlemlerinin gerçekleştirilmesi gibi manuel faaliyetleri azaltma veya ortadan kaldırma potansiyelini taşıdığı belirtilmektedir. Aynı rapora göre, kayıtların geriye dönük olarak değiştirilememesi, her işlemin birden fazla tarafça doğrulanması ve onaylanması gerekliliği bir yandan geleneksel sistemlere göre etkinliği azaltırken bir yandan da işlemlerde şeffaflığın artması, faaliyetlerin basitleşmesi ve yolsuzlukların en aza indirilmesi gibi avantajlar sunmaktadır.

Sheldon'a (2018) göre blokzincir iş sürekliliği ve felaket kurtarma planlaması konusundaki faaliyetleri iyileştirme ve bu alandaki endişeleri giderme potansiyeline sahiptir. Blokzincir ile veriler kalıcı bir kayıt defteri biçiminde depolandığından ve ağdaki her bir düğüm tarafından özdeş kopyalar tutulduğundan veri yedekleme ihtiyacı ortadan kalkabilecektir.

Herkese açık bir blokzincir olan Bitcoin örneğinde olduğu gibi, coğrafi olarak farklı birçok bölgedeki düğümlerde tutulan kayıtlar, herhangi bir coğrafi bölgede yaşanacak bir felaket durumunda çalışmaya devam edeceğinden ayrıca bir felaket kurtarma ya da iş sürekliliği tasarımına gerek duyulmayacaktır.

Ramachandran ve Rehermann (2019) özellikle finans sektöründe çok sıkı kurallarla sınırları çizilmiş olan, kara paranın aklanmasının önlenmesi, vergi kaçakçılığının engellenmesi ve müşterini tanı yükümlülüğü gibi riskten arındırma faaliyetlerinin bazen sermaye akışını engellemeye hizmet edebildiğini belirterek bu düzenlemelerin özellikle kendi ülkelerindeki yakınlarına para göndermek isteyen göçmenler, insani yardım sağlayan sivil toplum kuruluşları ve az gelişmiş ülkelerdeki küçük ve orta ölçekli işletmeler için kayıplara neden olduğunu öne sürmektedir. Blokzincir teknolojisi mevzuata uyum maliyetlerini azaltıp şeffaflığı artırarak bu kayıpları önleyebilecektir. Örneğin; Müşterini Tanı yükümlülüğünün finans kuruluşlarına yıllık maliyeti ortalama 60 milyon $'dır. Bazı büyük kuruluşlar müşterilerin doğrulanması için yılda 500 milyon $ harcamakta, bu doğrulama işlemi aylarca sürebilmektedir. Blokzincir teknolojisi bu maliyetleri azaltma ve doğrulama süresini büyük oranda kısaltma potansiyeline sahiptir.

Niforos'a (2017) göre, mali bilgilerin blokzincir teknolojisi ile saklanması manuel denetimden kaynaklanan hataları ortadan kaldıracak, etkinliği artıracak, raporlama maliyetlerini düşürecek, daha etkin ve sürekli denetimi kolaylaştıracaktır. Ayrıca, kara paranın aklanmasının önlenmesi ve müşterini tanı yükümlülüklerini yerine getirmek için bankaların katlandığı çok yüksek maliyetleri düşürme potansiyeline de sahiptir.

Birleşik Krallık Devlet Bilim Ofisi tarafından hazırlanmış olan "Blokzincirin Ötesinde Dağıtık Kayıt Defteri Teknolojisi" başlıklı raporda Walport (2016) mevcut veri yönetim sistemlerinin genellikle tek bir merkezde kurulmuş eski bilgi teknolojileri sistemlerinden oluştuğunu, bu sistemlerin dış dünyayla iletişimlerinin bir dizi ağ ve mesajlaşma sistemleri eklenerek sağlanabildiğini ve bu ilavelerin de maliyeti ve karmaşıklığı artırdığını öne sürmektedir. Merkezi sistemler siber saldırılara karşı daha duyarlıdır ve tek nokta hata maliyetleri yüksektir. Ayrıca, merkezi sistemler ile bunların yedekleri genellikle senkronize ve güncel değildir. Dağıtık kayıt defteri teknolojisi ise yapısal olarak tek bir veri tabanı yerine aynı kayıt listesinin paylaşılan çok sayıda kopyasını içermesi nedeniyle saldırılara karşı daha güçlüdür. Bir siber saldırının başarılı olması için kayıt defterinin tüm kopyalarına

saldırmak zorunludur. Bu teknoloji aynı zamanda yetkisiz veri değiştirme veya tahrifata karşı da dayanıklıdır. Ağdaki katılımcılar kayıt defterinin herhangi bir yerindeki değişiklikten derhal haberdar olurlar.

Walport (2016: 65) uygun biçimde tasarlanması halinde bu teknolojinin yaratacağı fırsatları operasyonel maliyetlerin, ödemelerdeki hata ve usulsüzlüklerin azalması, işlemlerde şeffaflığın artması, bankacılık sistemine erişimi olmayan insanların finansal hizmetlere erişebilmesi, vatandaşların verilerinin korunmasının maliyetini düşürmesi, küçük ve orta ölçekli işletmelerin büyümelerini ve finansman bulmalarını kolaylaştırma olarak sıralamaktadır.

Dai'ye (2017: 60, 61) göre blokzincir teknolojisinin nesnelerin interneti gibi diğer bazı teknolojilerle birlikte kullanılmasıyla fiziksel varlıkların hareketlerinin de gerçek zamanlı olarak izlenebilmesi mümkündür. Bu özelliği ile neredeyse gerçek zamanlı olarak kullanıcı rolleri ve taleplerine göre blokzincir kayıtları ilgili taraflara sürekli olarak yayınlanabilmektedir.

İngiltere Çalışma ve Emeklilik Müsteşarlığı tarafından her yıl yapılan sosyal yardım tutarı 166 milyar £ olup bunun yaklaşık 2,6 milyar £'luk kısmı işlem hatası ve yolsuzluk gibi nedenlerle kaybedilmektedir. Mevcut vergi sistemindeki hata ve yolsuzluklarla birlikte hedefine ulaşmayan yardım tutarı 5 milyar £'u aşmaktadır. Ayrıca, yapılan sosyal yardımların hedefler doğrultusunda harcanıp harcanmadığı izlenememektedir. Blokzincire dayalı dijital kimliklerin kullanılması yardımlara daha düşük maliyetlerle erişimi sağlayarak amaç dışı ve usulsüz kullanımları engelleyecektir (Walport, 2016: 67).

Dünya Bankasına göre, 2018 yılı itibariyle dünya üzerinde temel kimlik belgesi olmayan insan sayısı yaklaşık 1 milyardır. Genellikle en yoksul ve en korunmasız gruplar içerisinde olan bu insanların çoğunluğunu az eğitimli, marjinalleştirilmiş kadın ve kız çocuklar, göçmenler, mülteciler, sığınma hakkı isteyenler, engelliler ve kırsal kesimde yaşayanlar oluşturmaktadır. Blokzincir teknolojisinin hiçbir resmi kaydı olmayan bu insanlarla ilgili bazı fırsatlar yaratacağı düşünülmektedir (World Bank, 2019).

Mevcut yapıda devletler ve işletmeler tarafından sunulan ürün ve hizmetlere ilişkin veriler büyük oranda merkezi sunucularda, bulut ortamında ya da basılı kâğıt ortamında, büyük

yığınlar halinde saklanmaktadır. Yönetim ve işletim bakımından avantaj sağlamakla birlikte bu merkezi yapı veriyi saldırıya açık hale getirmektedir. Blokzincir tasarımı ile kayıtların dağıtık bir biçimde saklanması özellikle kaba kuvvet saldırılarına karşı korunma sağlamaktadır.

Blokzincir teknolojisi ile birlikte finans sektörünün gündemine girmiş olan ifadelerden biri de İlk Dijital Para Arzıdır (Initial Coin Offering - ICO). ICO blokzincir teknolojisinin ve kripto para birimlerinin seçkin bir yeniliği, kitlesel fonlama ve sermaye toplamak için yeni bir yöntemdir. Token satışı olarak da bilinen ICO bir kuruluşun yazılım geliştirme, iş operasyonları, iş geliştirme veya benzer girişimleri finanse etmek amacıyla dijital tokenların satılmasıdır. Arz esnasında alıcılar genellikle belirli bir kriptografik adrese fiyat para ya da kripto para birimi cinsinden katkıda bulunur ve katkıları karşılığında belirlenen satış fiyatına göre token sahibi olurlar (Stellar Development Foundation; The Luxembourg House of Financial Technology, 2017). Halka açık olan satışta herkes bir token alıcısı olabilir. Satın alma motivasyonu tokeni çıkarılma amacına göre kullanmak veya ticari kazanç elde etmek olabilir. ICO'lar sağladıkları fayda kadar bazı riskleri de içinde barındırmaktadır. Bu nedenle birçok ülkede yasal düzenlemelere tabidir.

Devletler, sosyal güvenlik numarası, vergi bilgileri, kullanılan oylar ve kimlik bilgileri gibi vatandaşlarının en kıymetli bilgilerini korumakla mükelleftir. Blokzincir teknolojisinin kamu hizmetlerinde kullanılması bu hassas bilgilerin korunmasına dair yaşanan güven ve şeffaflıkla ilgili sorunların üstesinden gelinmesi, veri koruma ve gizlilik konusundaki ihtiyaçların giderilebilmesi bakımlarından fırsat sunmaktadır. Devletler, farklı birimlerde tutulan benzer ancak özdeş olmayan veriler, birlikte çalışabilirlik sorunları ve şeffaflıkla gizliliği muhafaza etmek arasındaki dengenin sağlanması ihtiyacı gibi konular nedeniyle ellerindeki bu kıymetli verilerin potansiyelinden tam faydalanamamaktadır. Blokzincir teknolojisi bu potansiyelin açığa çıkması için önemli bir fırsattır.

Blokzincir teknolojisinin yapısal özelliklerinden kaynaklanan, kendine özgü güçlü yanları ve getirdiği avantajlar aşağıdaki biçimde özetlenmektedir:

- Aracıya gerek duyulmayan, dağıtık bir güven ortamı
- Şeffaflık
- Güvenlik

- Sistemik hatalara ve dışarıdan müdahaleye dayanıklılık
- Eklenen verilerin silinememesi, değiştirilememesi
- Düşük işlem maliyetleri
- Tek nokta hatasını ortadan kaldırma
- Yolsuzluk ve hataların azaltılması
- Finansman sağlama kolaylıkları (ICO)
- Yeni pazar ve gelir alanları yaratma (örneğin kriptoparalar)
- Hızlı ve her an (24 saat) gerçekleştirilebilir işlemler
- Manuel işlemleri azaltma, doğrulama ve denetim faaliyetlerini kolaylaştırma
- Diğer sektörlere ve teknolojilere de kazanç sağlama imkânı
- Arıza süresi sıfır olan bir sistem sunması
- Çok küçük miktarlı transfer işlemlerinin (mikro ve nano ödemeler) gerçekleştirilebilmesi
- Mevzuata uyum maliyetlerinin azaltılması (Örneğin KYC ve AML)
- Bankacılık sistemine erişimi olmayan insanların finansal hizmetlere erişebilmesi
- Veri koruma maliyetlerinin düşürülmesi
- Küçük ve orta ölçekli işletmelerin büyümelerini ve finansman bulmalarını kolaylaştırma
- Sosyal yardımların daha düşük maliyetle dağıtılması, amaç dışı ve usulsüz kullanımının engellenmesi
- Kurumlar arasında güvenli veri paylaşımı
- Kendi verisini yönetme yetkisinin bireylere verilmesi

2.1.7. Blokzincirin zayıf yönleri ve tehditler

Yaga, Mell, Roby ve Scarfone'a (2018: 34) göre büyük miktarda verinin belgeler, görüntüler, video ve uygulamalar gibi farklı biçimlerde depolanması için veri tabanları kullanılırken blokzincir daha çok bir işlemler listesidir ve çoğunlukla akıllı sözleşmeleri çalıştırmak için küçük veri parçalarını içerirler. Blokzincir genel tasarımı itibariyle genel veri depolamaya uygun değildir.

Smith'e göre (2018) blokzincir teknolojisinin finans ve sağlık gibi kritik sektörler için cazibe kazanması için veri güvenliği, veri gizliliği, uzman havuzunun yetersizliği, mevzuat düzenlemelerinin eksikliği gibi problemler giderilmelidir.

Cambridge Üniversitesi, Alternatif Finans Merkezi tarafından Visa ve Ernst&Young firmalarının desteği ile Aralık 2016 ile Mayıs 2017 arasında yapılan, 49 farklı ülkeden 200'ün üzerinde kamu ve özel sektör temsilcisinin dâhil edildiği çalışmada blokzincir teknolojisinin kabulünün önündeki engeller yasal riskler ve düzenleyici çerçevenin olmaması, gizlilik ve güvenlik endişeleri, mevcut iş süreçlerinin değiştirilmesi konusundaki isteksizlik, teknolojinin henüz olgunlaşmamış olması, iş ağının geliştirilmesinin güçlüğü, veri koruma yasalarından kaynaklanan potansiyel problemler, ölçeklenebilirlik ve performans kaygıları, kontrolü elden bırakma konusunda gönülsüzlük, bilinmeyen fayda/maliyet, uygun kullanım durumları ve senaryolarının yetersizliği olarak sıralanmaktadır (Hileman ve Rauchs, 2017).

Moreno ve Lomaquiz (2020) blokzincir teknolojinin uygulamalarından biri olan İlk Dijital Para Arzı (ICO) risklerini spesifik mevzuatının bulunmaması, fiyat oynaklığı ve likidite riskleri, usulsüzlük olasılığı, ilgili bilgilere uygun olmayan erişim, projelerin henüz başlangıç aşamasında olması, teknolojik ve altyapıya bağlı arıza ve aksaklık olasılığı ve işlemlerin doğası gereği uluslararası olması biçiminde aktarmaktadır.

Salmon ve Myers (2019) bokzincir teknolojisinin temel risklerini birden fazla yetki alanına dağılmış olan, yönetişimi güç yapı, veri koruma, mahremiyet ve gizlilik düzenlemelerine uyum ve siber saldırılar olarak sıralamaktadır. Proje fikirleri için fon toplamak amacıyla kripto varlık çıkarmak isteyen işletmelerin sayısı sürekli olarak artmaktadır ve bu fon toplama sürecine ilişkin yasal düzenlemeler konusunda bir standart ya da uluslararası net bir yaklaşım bulunmamaktadır. Birçok uygulayıcı ve akademisyene göre blokzincir teknolojisi AB Genel Veri Koruma Yasası (GDPR) gibi gizlilik düzenlemelerine uyumsuzdur. Özellikle izin gerektirmeyen blokzincir ağlarında tüm kullanıcılar ağdaki veriye erişebilmektedir. Bu ağların merkezi bir yönetimi ya da sahibi de olmadığından bu yasaların uygulanmasının dayatılması için bir mercii bulunmamaktadır. Blokzincir ağı tüm dünyaya açık olduğundan gizli bilgilerin ülke dışına çıkarılması mevzuat bakımından bir diğer problemdir. Veri güvenliği gelişmiş şifreleme teknikleri ile ileri düzeyde sağlanmış olmakla birlikte, kullanıcıların kriptografik anahtarları uygun biçimde saklamaları gerekliliği de düşük de olsa bir risk noktası olarak değerlendirilmektedir. Siber güvenlik ile ilgili riskler ise kaba kuvvet saldırıları, DDoS saldırıları, çifte harcama, akıllı sözleşmelerdeki program kodlarını hedef alan saldırılar olarak sıralanmaktadır.

Finck (2018), GDPR veri sahibi haklarını blokzincir bağlamında analiz ettiği çalışmasında verinin korunması ile ilgili GDPR hükümleri ile blokzincir teknolojisi ilişkisini Çizelge 2.4'te verildiği biçimde yorumlamaktadır.

Çizelge 2.4. GDPR veri sahibi haklarının blokzincir kapsamında analizi (Finck, 2018)

GDPR konusu	**Blokzincirde "veri sahibi" haklarının analizi**
Veri minimizasyonu	GDPR, kişisel verilerin "belirli, açık ve meşru amaçlar için toplanmasını ve bu amaçlarla uyumlu olmayan bir şekilde daha fazla işlenmemesini" zorunlu kılar. Blokzincir sürekli büyüyen değişmez bir veri tabanıdır ve ağdaki birden çok düğümde dağıtılır. Bu özellikler, veri minimizasyonunun uygulanmasında zorluklar yaratır.
Değişiklik hakkı	GDPR, kişisel verilerin doğru ve güncel olmasını gerektirir. GDPR'a göre işlendikleri amaçlar dikkate alınarak yanlış olan kişisel verilerin gecikmeden silinmesi veya düzeltilmesini sağlamak için her makul adım atılmalıdır. Veri sorumlusu bu nedenle kişisel verilerin düzeltilmesi için tüm düğümleri ele almalıdır. Ancak veri sorumlusu veri depolayan blokzincir düğümlerinin herhangi biri ya da tamamını tanımlayamaz. İlaveten, veri sorumlusu tüm düğümleri bilse bile, blokzincirin değiştirelemezlik özelliği nedeni ile düğümler veri silemez.
Unutulma hakkı	GDPR madde 17'de veri sahibinin kendisiyle ilgili verilerin herhangi bir gecikme olmaksızın silinmesini talep etme hakkı vardır. Blokzincirin kayıtların değiştirirlememe özelliği bu maddeyi uygulamayı zorlaştırmaktadır.
Erişim hakkı	Blokzincirde, veriler genellikle şifrelenmiş ya da hash biçiminde olduklarından genellikle bloklar içinde hangi verilerin depolandığı bilinmez. GDPR Madde 15'e göre veri sahibi kişisel verilerinin işlenip işlenmediğini öğrenme hakkına sahiptir. Blokzincirde bunun yolu veri sahibinin izin gerektirmeyen ağa katılarak blokzincirin bir kopyasını elde etmesidir. Ancak bunun GDPR bakımından tatmin edici bir çözüm olup olmadığı belirsizdir. Yine Madde 15'te veri sahiplerinin, verilerin üçüncü ülkelere aktarıldığı durumlarda güvenlik önlemleri hakkında bilgilendirilme hakkına sahip oldukları belirtilmektedir. Blokzincirde coğrafi konumdan bağımsız olarak veriler tüm düğümlere dağıtılmaktadır. Madde 15(3)'e göre, veri sahiplerinin işlenmekte olan kişisel verilerinin bir kopyasını alma hakları vardır. Ancak blokzincirde veriler kriptografik olarak takma adlarla tutulduğundan imkansızdır.

Niforos (2019) blokzincir teknolojisinin yaygın biçimde benimsenmesinin önündeki engelleri teknik, organizasyonel ve düzenleyici olmak üzere üç sınıfa ayırmakta, potansiyel problemleri; blokzincir ağının genişlemesinin neden olacağı işlem gecikmesi ve veri depolama gereksiniminden kaynaklanacak ölçeklenebilirlik sorunları, yeterli olgunluk düzeyine erişilememesi nedeniyle siber güvenlik kaygıları, endüstri standartlarının henüz olmaması nedeniyle farklı blokzincirlerin birlikte çalışmasında yaşanacak problemler, veri mahremiyetinin sağlanmasında unutulma hakkı, anonimliğin korunması gibi konuları da içeren mevzuata uyuma ilişkin soru işaretleri, yasal düzenlemelerin teknolojinin hızına yetişememesi, mevcut Müşterini Tanı ve Kara Paranın Aklanmasının Önlenmesi düzenlemelerine uyum güçlüğü, yüksek yatırım maliyeti olarak sıralamaktadır.

Birleşik Devletler Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından yayınlanmış olan Blokzincir Teknolojine Genel Bakış başlıklı raporda değiştirilemezlik özelliğinin blokzincir teknolojisinin hem en temel ve en faydalı özelliği, hem de pratik uygulamalar için en önemli kısıtlılığı olduğu belirtilmektedir. Geleneksel veri tabanlarından farklı olarak blokzincire eklenen kayıtların silinmesi ya da değiştirilmesi mümkün değildir. Bu nedenle, bu özelliğin kullanılmak istenen alan için bir mani teşkil edip etmediği dikkatli biçimde değerlendirilmelidir (Yaga ve diğerleri, 2018: 34).

Berryhill ve diğerleri (2018) tarafından hazırlanan Blokzincir Teknolojisi ve Kamu Sektöründe Kullanımı konulu OECD raporunda blokzincir teknolojisinin kamu hizmetlerinde kullanımı konusundaki güçlükler ve sınırlılıklar aşağıdaki biçimde listelenmektedir:

- Değiştirilemezlik: Blokzincirin hem en temel ve faydalı özelliği, hem de bazı uygulamalar için en önemli kısıtlılığıdır. Karar vericiler blokzincirin bu özelliğinin uygulama alanı için bir avantaj mı yoksa kısıtlılık mı olduğunu değerlendirmelidir.
- Şeffaflık, gizlilik ve dağıtıklık: İzin gerektirmeyen, herkese açık blokzincirler kusursuz bir şeffaflık gösterirler. Kişisel bilgilerin depolanmasının muhtemel olduğu durumlarda gizlilik ve mahremiyet en önemli önceliktir. Yasal düzenlemeler bu tip bilgilerin korunması konusunda çok katıdır. GDPR'ın blokzincir teknolojisi açısından sonuçları henüz tam olarak anlaşılamamıştır. Dağıtık defter teknolojileri (DLT) ile veri koruma kanunlarının etkileşimleri detaylı analizler gerektirmektedir. Dağıtık karar verme ve gizlilik ayarlarının düzeyi konusunda birini seçerken diğerinden feragat etme durumu söz konusudur. Yüksek düzeyde gizlilik çok daha resmi yönetişim modellerini (izin gerektiren blokzincirler) gerektirmektedir. Radikal şeffaflık ise kişisel verilerin açığa çıkması riskini ortaya çıkarmaktadır.
- Veri depolama: Kamu ve özel sektör kuruluşları genellikle büyük miktarda veriyi belgeler, görüntüler, videolar ve uygulamalar gibi farklı biçimlerde depolamak için veri tabanları kullanmaktadırlar. Blokzincir ise daha genel olarak bir işlemler listesidir ve çoğunlukla akıllı sözleşmeleri yönlendirmek ve çalıştırmak için küçük veri parçalarını içerirler. Genel veri depolama için tasarlanmamıştır. Eğer devlet kuruluşları sadece veri depolama için bir çözüm arıyorsa blokzincir teknolojisi uygun olmayabilir. Bununla birlikte, eğer işlem kayıtlarının güvenilir ve dağıtık biçimde yürütülmesi hedefleniyorsa blokzincir teknolojisi uygulanabilir bir çözümdür. İhtiyaçları giderecek hibrit bir

yaklaşım da pekâlâ mümkündür. Blokzincir teknolojisi ve veri depolama çözümü birlikte kullanılabilir. Zincirin dışında tutulan ve başka bir yerde depolanan veri ile blokzincir işlemlerinin birbirlerine bağlanması (link) sağlanabilir.

- Veri kalitesi: Geleneksel bilgi sistemlerinde olduğu gibi girdi olarak kullanılan kaynak verinin kalitesi blokzincir üzerindeki veriyi ve bu veriden türetilen sonuçların kalitesini doğrudan etkilemektedir. Bir diğer deyişle, girdi noktasındaki doğru, zamanlı ve güvenilir olmayan veriyi hiçbir analitik işlem telafi edemez.
- Kodlama ve yönetişim modelleri: Blokzincir teknolojisinin en çok zikredilen faydalarından biri merkezi otoriteye olan gereksinimi ortadan kaldırmasıdır. Bununla birlikte, herkesin erişim sağlayarak işlem yapabildiği izin gerektirmeyen kayıt defterleri için bile bu tam olarak doğru değildir. Blokzincirler kod geliştiriciler, madenciler, platformunun geliştirilmesinde kilit rol oynayan diğer karar vericiler tarafından inşa edilmekle birlikte blokzincirin içerisine kodlanmış olan yapılar, aksiyonlar ve altında yatan kararlar gerçekleştirilen işlemler kadar şeffaf olmayabilir.
- Blokzincir konusundaki olumsuz yargılar: Blokzincire ilişkin yaşanan en büyük güçlük teknolojiyi vatandaşlara anlatmanın zorluğu, teknolojinin karmaşıklığı, yanlış anlaşılması ve konu hakkındaki eğitimin yetersizliğidir. Blokzincir teknolojisinin güveni artıracağı düşünülmektedir ancak gerek devlette gerekse blokzincir topluluğu içinde yapısal bir güvensizlik bulunmaktadır.
- Maliyetler: Bu teknolojiyle ilgili yüksek kısa dönemli maliyetler geniş çaplı kullanımını engellemektedir. Bu maliyetler özellikle firmalar için ürkütücü olmakla birlikte devlet tarafından yürütülen blokzincir projelerinde de ilk yatırımlar tartışılmalı ve fayda-maliyet analizi yapılmalıdır. Piyasada göreceli olarak yeni olan "hizmet olarak blokzincir" (blockchain as a service) çözümleri daha hızlı ve daha kolay deneyimlere olanak sağlamaktadır.
- "İş İspatı" mutabakat modeli ile ilgili sorunlar: İzin gerektirmeyen blokzincirlerde yeni blok eklenmesi için en yaygın olarak kullanılan metot İş İspatı (Proof of Work) mutabakat modelidir. Bununla birlikte, kamu sektörü uygulamalarında izin gerektiren blokzincirler ve bunlara uygun olan Otorite İspatı (Proof of Authority) gibi modellerin kullanılması daha uygun ve muhtemeldir. Çünkü bu modelde bir blokzincire erişmek ve yeni bilgi eklemek için role dayalı izinler verilir. Özellikle Bitcoin platformundaki madencilik süreci ve İş İspatı mutabakat modeli çok yüksek miktarda elektrik harcanmasını gerektirmektedir. Bununla birlikte, bu aşırı elektrik tüketimi yalnızca İş

İspatını kullanan blokzincir platformları için söz konusudur. Kamudaki uygulamaların çok büyük bölümü başta Otorite İspatı olmak üzere enerji tüketiminin bir problem yaratmadığı farklı mutabakat mekanizmaları kullanacaklardır.

- Ölçeklenebilirlik: İş İspatını kullanan izin gerektirmeyen blokzincirler kullanılışlılıklarını kısıtlayan ölçeklenebilirlik problemi ile de karşı karşıyadır. Bu durum, platformun işlemleri gerek duyulan hızda yerine getirememesi ve bir süre sonra maksimum işlem kapasitesine ulaşmasını ifade etmektedir. Özellikle Bitcoin gibi mevcut platformlarda bu problem mevcuttur. Bitcoin saniyede yalnızca yedi işlem gerçekleştirme kapasitesine sahiptir ve bu hız Visa (saniyede 1.667 işlem) veya PayPal (saniyede 193 işlem) gibi geleneksel finans şirketleri ile rekabet edecek düzeyde değildir.

ITU-T (2019a) dağıtık kayıt defteri teknolojisinin kullanım senaryoları konulu raporunda dağıtık kayıt defteri teknolojilerinin uygulanması ve kabulü önündeki engeller teknolojik riskler, bilgi riskleri, ekosistem engelleri, yapısal özellikler ve yasal engeller olmak üzere beş ana sınıfa ayrılmış olup bunların detaylarını aşağıdaki biçimde listelemektedir:

- Genel teknolojik riskler
  - Temel teknoloji ve eski altyapı: Büyük endüstriler tarafından kullanılan finans, sigorta, kimlik yönetimi gibi eski sistemleri güncellemek ya da değiştirmenin, yeni bir altyapı oluşturmanın, gerekli becerilere sahip yeni personelin temini için hem zaman hem de sermaye gerekmektedir. Eski ve yeni sistemi birlikte kullanmanın getireceği ek bir maliyet ve karmaşıklık da bulunmaktadır.
  - Blokzincir üçlü çelişkisi: Dağıtık kayıt defterleri merkezsizlik, ölçeklenebilirlik ve güvenlik olmak üzere üç temel özelliğe sahiptir. Ancak, bu üç özellikten aynı anda yalnızca ikisi sağlanabilmektedir. Bu durum blokzincir üçlü çelişkisi olarak adlandırılmaktadır. Blokzincir teknolojisi kullanılırken uygulama önceliklerinde bu çelişki dikkate alınarak örneğin, ölçeklenebilirlik ve güvenlik için merkezsizlikten, merkezsizlik ve güvenlik için ölçeklenebilirlikten feragat edilmek durumunda kalınmaktadır. Bu özellik, blokzincir çözümlerinin benimsenmesini olumsuz etkilemektedir.
  - Standartların bulunmaması: Hâlihazırda birçok farklı platform bulunması ve geniş kabul görmüş, farklı platformlar arasında birlikte çalışabilirliği sağlamaya yardımcı standartların bulunmaması bir dezavantaj olarak değerlendirilmektedir.

- Veri güvenliği: Herkese açık blokzincirler veri güvenliği endişesi oluşturmaktadır. Uygulama ve düzenlemelere bağlı olarak bazı verileri şifrelenmemiş bir kayıt defterinde tutmak imkânsız veya yasadışı olabilir. Herkese açık dağıtık bir sistemde şifrelenmiş verilerin tutulması maliyetlidir. Şifreleme teknolojilerinin gelişmesi, sıfır bilgi kanıtları ve çok taraflı hesaplama gibi unsurlar bu sorunu çözme potansiyelini taşımaktadır.
- Bazı hata noktalarının varlığını koruması: Bitcoin gibi kripto paraların kullanıcıları fiyat para kripto para dönüşümlerini gerçekleştirmek ve işlemleri kolaylaştırmak için borsalar ve cüzdan yazılımlarını kullanmaktadırlar. Bu borsalar ve cüzdan sağlayıcıları mevcut sistemdeki güvenilir üçüncü taraflarla aynı özellikleri taşımakta, dahası, yasal düzenlemeleri henüz tam olarak yerleşmediği için dolandırıcılık ve yolsuzluk riski taşımaktadırlar. 2013 yılında tüm Bitcoin işlemlerinin %70'inden fazlasını gerçekleştiren bir borsa olan Tokyo merkezli MtGox olayı bu duruma bir örnek olarak gösterilebilir. 2014 yılında firma 450 milyon $ değerinde Bitcoin kaybedildiğini açıklayarak iflas başvurusunda bulunmuş, kaybedilen paraların yalnızca %24'ü kurtarılabilmiştir.
- Yatırım geri dönüşü: Kullanıcılar tarafından tereddütlü yaklaşılması ve yavaş benimsenmesi nedeniyle bu teknolojiye dayalı projeler diğer teknolojilere kıyasla daha yavaş bir yatırım getirisi sergilemektedir.
- Potansiyel yüksek uygulama maliyeti: İlk uygulamanın potansiyel yüksek maliyetleri, erken benimsemeye ilişkin algılanan riskler ve mevcut uygulamaların kesintiye uğrama olasılığı teknolojiye bakışı olumsuz etkilemektedir.
- Mahremiyet riskleri: Mahremiyet blokzincirin güçlü yönü olmakla birlikte, verilerin herkese açık ağlarda paylaşılmasının doğurduğu mahremiyet endişelerinin giderilmesi için mevcut ve gelecekteki şifreleme yöntemlerinin kullanıcı mahremiyetini koruma konusunda yeterince güçlü olması sağlanmalıdır. Özellikle kişisel verileri içeren uygulamalar için bu riskler önemli boyuttadır. Kişisel bilgilerin kaydedildiği durumlarda gizlilik ve mahremiyet en önemli öncelik olup yasal düzenlemeler bu tip bilgilerin korunması konusunda çok katıdır. Bu nedenle, açık ağlarda veri paylaşan blokzincir uygulamalarında kullanıcı gizliliği ve mahremiyetinin sağlanması garanti edilmelidir.

- Bilgi riskleri
  - Eğitim – Dağıtık Kayıt Defteri Teknolojileri konusunda genel bilgi: Bu teknoloji, hem kendi özellikleri hem de potansiyel iş değeri açısından anlaşılması zor, geniş ve

karmaşık bir konudur. Bazı durumlarda herhangi bir problemin blokzincir ile çözülebileceği algısı bulunmaktayken bazı durumlarda da bu teknolojiden yararlanılabilecek karmaşık sistemlerde bilgi ve anlayış eksikliği nedeniyle teknoloji benimsenmemektedir. Teknolojiyi çok iyi anlayan ancak iş ve operasyon gereksinimlerini anlamayan blokzincir geliştiricileri ile işi anlayan ancak blokzincirin nereye değer katabileceğinin farkında olmayan işletme sahipleri arasındaki uçurumun giderilmesi için karşılıklı eğitim şarttır.

- Eğitim – Spesifik bilgi: Dağıtık Kayıt Defteri Teknolojileri, kripto paralar ve tokenlar arasındaki farkın anlaşılmaması alandaki önemli engellerden biridir.
- Kötü itibar – yolsuzluklar ve siber saldırılar: Bankalar ya da diğer aracılara ihtiyaç duymadan ve fiziksel paraya ihtiyaç olmadan fon transferinin gerçekleştirilebilmesi dağıtık kayıt defteri teknolojilerinin İpek Yolu (Silk Road) olarak bilinen yasadışı çevrim içi uyuşturucu ve illegal madde ticareti için kullanılmasına neden olmuştur. Özellikle Bitcoin'in merkezi olmayan ve anonim yapısı yasadışı faaliyetler için cazip hale gelmesini sağlamıştır. Bu olumsuz çağrışım blokzincir teknolojisinin benimsenmesini engellemiş, zamanla yasadışı işlemlerin kapsamı azalmasına karşın kötü itibarın ortadan kalkması zaman almıştır. Blokzincir teknolojisinin fon toplama, ilk halka arz veya risk sermayesi fonları yoluyla finansman sağlama amaçlı kullanılmasında yaşanan çok sayıda dolandırıcılık ve siber saldırı da teknolojiye olan güveni olumsuz etkilemiştir.
- Uzmanlığın oluşumu ve kullanımı: Çok sayıda farklı blokzincir platformunun ortaya çıkması ekosistemin dağılmasına, araştırma, geliştirme ve uygulama alanlarında gereken uzmanlık düzeyine ulaşmak için gerekli bilginin parçalanmasına neden olmuştur.
- Merkezi olmayan yönetişim mekanizmaları konusundaki yetersiz deneyim: Merkezi sistemlerin aksine dağıtık kayıt defteri sistemleri ağdaki katılımcıların tamamı ya da bir kısmı tarafından yönetilir. Blokzincir platformlarında ve akıllı sözleşmelerde bu yeni yapı yazılım geliştiriciler, ağ katılımcıları, madenciler, işlem gerçekleştirenler ve işlemleri doğrulayanlar gibi yeni kavramlar ve yönetişim yapısı getirmiştir.

- Ekosistem engelleri
  - Baskın platformlar – izin gerektiren ve izin gerektirmeyen platformların mücadelesi: Dağıtık kayıt defteri teknolojileri kullanılan mutabakat mekanizmasına göre izin gerektiren veya izin gerektirmeyen olarak farklılık gösterir. Bazı durumlarda bu iki yaklaşım birlikte de kullanılabilmektedir. Mevcut çözümlerin kalitesini

değerlendirmek ve bunları mevcut bilgi teknolojileri ortamlarına entegre etmenin en iyi yolunu belirlemek zordur.

- Çok sayıda alternatif çözüm: Dağıtık kayıt defteri teknolojisi her zaman belirli bir sorun için en iyi çözüm sağlamayabilir. Bazı durumlarda geleneksel merkezi çözüm daha iyi bir seçim olabilmektedir. En iyi çözüme karar vermek hem zaman alıcıdır hem de konu hakkında iyi düzeyde bilgi sahibi olmayı gerektirmektedir.
- Birlikte çalışabilirlik – Farklı dağıtık kayıt sistemlerinin birlikte çalışamaması: Hepsi temelinde dağıtık kayıt defteri teknolojisi olsalar da farklı platformlar birbirleri ile sorunsuz biçimde konuşamamaktadır.
- Yetersiz kullanıcı arayüzü (front-end) gelişimi: Bir ürünün kullanım kolaylığını tanımlayan önyüz ya da ön ucun yetersiz ya da karmaşık olması, konu hakkında teknik bilgisi yetersiz olan kişilerin uygulamaları kullanmasını ve benimsemesini güçleştirmektedir.
- Aracının ortadan kaldırılması: Dağıtık kayıt defteri teknolojisinin mevcut aracıları ortadan kaldırma ya da bunlara olan ihtiyacı azaltma potansiyeli bu aracıların kendilerini tehdit altında hissetmelerine neden olacak, rollerin, hiyerarşinin ve organizasyon yapısının yeniden tasarlanmasını gerektirecektir.
- Dağıtık kayıt defteri sağlayıcısının güvenilirliği: Birçok platform ve hizmet sağlayıcı henüz yatırım arayışında olan, finansal istikrarı denenmemiş, ürün yol haritaları belirsiz olan yeni girişimlerdir. Bu nedenle bu sağlayıcılara mesafeli yaklaşılmaktadır.

- İçsel özellikler
  - Değiştirilemezlik: Operasyonel bir dağıtık kayıt defterinde akıllı sözleşmeler geliştirilirken bir arıza ya da hatayı daha sonra düzeltme şansı bulunmamakta, hatalı kodla oluşturulan değiştirilemez kayıtlar silinememektedir.
  - Büyük platformları yükseltme ya da geliştirme güçlükleri: Merkezi olmayan sistemler, platformu yükseltmek için tüm katılımcıların onayını almalıdır. Yeni gizlilik ve ölçeklenebilirlik özelliklerinin tanıtılması gibi basit görevler, merkezi sistemlere kıyasla çok daha karmaşık olabilmektedir. Riskler arasında ayrılma oranı, katılımcıların hareket etme isteksizliği vb. yer almaktadır.
  - Yeni siber saldırı çeşitleri
  - Yüksek enerji tüketimi: İş İspatı gibi mutabakat protokolleri yüksek miktarda elektrik tüketimi gerektirmektedir.

- Yasal hususlar: Yasal düzenlemelerdeki eksiklik ve bazı konulardaki hukuki belirsizlik teknolojinin benimsenmesinin önündeki en büyük engellerden biridir.

Blokzincir teknolojisinin en temel ve en güçlü özelliklerinin başında kriptografi gelmektedir. Blokzincirde kullanılan şifreleme yaklaşımları günümüz için oldukça güçlü olsa da, kuantum bilişim alanındaki gelişmelerle birlikte şifreleme konusunda gelecekte çeşitli zafiyetler görülebileceği düşünülmektedir. Bu, blokzincir dünyası için hemen değil ama uzun vadede bir risk oluşturmaktadır. Blokzincir teknolojisi henüz çok yeni olduğundan bazı öngörülemeyen eksiklikler ve yazılım hatalarına rastlanabilmektedir. Siber saldırganlar için bulunmaz bir fırsat olan bu yazılım açıkları ciddi ekonomik kayıplara sebep olabilmektedir (Usta ve Doğantekin, 2017: 105, 108).

Blokzincir ağında hesaplara erişim şifresinin unutulması, hatalı işlem gerçekleştirilmesi gibi istenmeyen durumlar ortaya çıktığında bu durumu gidermek için başvurulabilecek bir merci, işlemleri iptal edecek ya da silecek bir mekanizma bulunmamaktadır. Kullanılan anahtarların saklanması kullanıcının sorumluluğundadır. Özel anahtarın kaybedilmesi, unutulması ya da çalınması halinde kullanıcının söz konusu varlığın sahibi olduğunu kanıtlaması mümkün değildir. Bu nedenle, özel anahtarın kaybedilmesi aynı zamanda bu anahtarla ilişkili varlığın da kaybedilmesi demektir. Psaila'ya göre (2017) yanlışlıkla veya bilinçli olarak hatalı ya da yetkisiz bir adrese değer transferi yapıldığında bu işlemi tersine çevirmek imkânsızdır. Blokzincir teknolojisini kullanan kuruluş bir oltalama saldırısına maruz kalırsa blokzincirin merkezi bir yönetimi olmadığı için bu olayın raporlanacağı bir dolandırıcılık birimi yoktur. Özel anahtar kaybedilirse bu anahtarla ilişkili hesaba (ve varlığa) erişim artık mümkün olmaz. Sheldon da (2018) kripto paraların ortak probleminin özel bir anahtarla ilişkilendirilmiş dijital varlıklara bu anahtarın kaybedilmesi halinde erişilememesi olduğunu belirtmekte, blokzincirin her sorunun çözümü olarak görülmemesi gerektiğini ve sağlayacağı katkının paylaşılan bir veri tabanı ya da ERP sisteminden fazla olduğundan emin olunmasının önemini vurgulamaktadır.

Blokzincir teknolojisine ilişkin hukuki düzenlemeler ve standartlar henüz gelişim aşamasındadır. Teknolojinin birçok farklı uygulama alanı olması, birçok farklı blokzincir çeşidinin ve platformunun bulunması, tamamen açık ve katılımı izne tabi olmayan blokzincir platformları üzerinde devletlerin kontrolünün çok kısıtlı olması gibi unsurlar mevzuat ve standart geliştirilmesini güçleştirmektedir.

Brender, Gauthier, Morin ve Salihi'ye (2018) ve Dai'ye (2017: 80) göre bir diğer önemli sorun ihtiyaç duyulan bant genişliğidir. Blokzincirde mutabakat algoritması ile doğrulanmadan önce işlemlerin tüm ağda dağıtılması gerekmektedir. Bu nedenle, kullanıcıların sayısı ve bunun sonucunda da işlem sayıları arttıkça daha güçlü bir ağ bağlantısı, büyük depolama kapasitesi ve etkin bir kayıt yönetimi yapısı gerekmektedir. Hâlihazırda, özellikle ticari işlemlerde gerek duyulan yüksek hacimli taleplere neredeyse anlık cevap verme konusunda mevcut veri tabanı sistemlerinin gerisindedir. Blokzincir teknolojisi genellikle önemli hesaplama ve depolama kaynaklarına ihtiyaç duyduğundan teknolojinin gelişimi depolama sistemlerinin, veri iletimi için bant genişliğinin ve işlemci gücünün gelişimi gibi bazı dış faktörlere bağımlıdır.

Brender ve diğerleri (2018) ölçeklenebilirliği bir sistemin boyutunda veya hacminde meydana gelen değişim sonucunda o sistemin fonksiyonlarını aynı biçimde sürdürebilmesi olarak tarif etmektedir. Katılımcı sayısı arttıkça blokzincir teknolojisinde ölçeklenebilirlik problemi ortaya çıkabilmektedir. Tasarımı gereği blokzincir ilk bloktan itibaren bütün işlemleri içerdiğinden kullanıcı ve işlem sayısı arttıkça blokzincirin boyutu da büyümektedir. Bitcoin platformunda saniyede yaklaşık 7 işlem gerçekleştirilebilmektedir. Ölçeklenebilirlik problemi daha çok herkese açık olan blokzincirler için geçerlidir. Ölçeklenebilirlik problemini gidererek saniyede binlerce işlem gerçekleştirebilen özel blokzincirler de mevcuttur. Ancak ölçeklenebilirlik sorununu çözmek için genellikle dağıtıklık ya da güvenlik özelliklerinden birinden feragat edilmesi gerekmektedir.

Blokzincir teknolojisi klasik sistemlerdeki güvenilir aracıya olan ihtiyacı ortadan kaldırıyor olsa da akıllı sözleşmelerin kullanımı gibi bazı durumlarda blokzincir sistemi dışından bazı güvenilir bilgilere erişilmesi gerekmektedir. Örneğin, hava sıcaklığına bağlı şartlar içeren bir akıllı sözleşmenin dikkate alacağı hava sıcaklığı değerinin güvenilir bir kaynaktan alınması gerekir. Sheldon (2018) blokzincir kullanılmaya başlandıkça eski sistemlerin ve üçüncü taraf bulut esaslı sistemlerin blokzincir ile bir arayüz oluşturacağını, sonuçta blokzincire yüklenen verileri üreteceğinden eski uygulamalar ve süreçlere ilişkin mevcut politika ve prosedürlerin devam ettirilmesi ve hatta daha da geliştirilmesi gerekeceğini öne sürmektedir. Blokzincirde kaydedilen veriler silinmeye ve değiştirilmeye karşı korumalı olsa da blokzincirin dışındayken genel bilgi teknolojisi risklerine karşı savunmasızdır.

Verilerin dış sistemden blokzincire aktarılmasındaki geçiş arayüzü bu yeni ortamdaki en hassas kontrol noktalarından biri olacaktır.

Başta Bitcoin olmak üzere bazı blokzincir platformlarında kullanılan ve İş İspatı olarak adlandırılan mutabakat mekanizması büyük enerji tüketimine sebep olmaktadır. Bu enerji tüketimi kendi başına bir sorun olmakla birlikte Bitcoin sisteminin sağlıklı ve güvenilir biçimde işleyişinin temelinde harcanan elektriğin getirdiği maliyet yatmaktadır. Tüketilen enerji karşılığında işlemlerin doğrulanması için bir teşvik mekanizması tasarlanmış olup doğrulama işlemi sonucunda bir ödül kazanılmaktadır. Sınırlı miktarda arz edilen kripto para durumlarında, teşvik sisteminin sona ermesi ile sistemin nasıl işleyeceği öngörülememektedir.

Sheldon'a (2018) göre blokzincir güçlü bilgi teknolojileri yönetişimine duyulan ihtiyacı değiştirmeyeceği gibi bazı durumlarda bu yönetişimi çok daha karmaşık hale getirecektir.

Blokzincir teknolojisinin kullanımında dikkate alınması gereken bir diğer konu bazı durumlarda birden fazla kuruluşla işbirliği içinde çalışma ihtiyacıdır. Bir blokzincir birden çok kuruluşa ait çok sayıda paydaşı içerebilir. Bu durumda, tüm paydaşların gereksinimlerinin karşılanıp karşılanmadığından emin olmak için birlikte çalışılması gerekmektedir (H. Rooney, Aiken ve M. Rooney, 2017).

Dai'ye (2017: 79) göre teknik bakımdan karmaşıklık, önemli miktarda finansal yatırım ve zaman gereksinimi, teknolojinin diğer paydaşlara yaygınlaştırılmasındaki güçlükler ve süreçlerde değişiklik gerekliliği gibi unsurlar, geçmişteki ERP ve EDI (Elektronik Veri Alışverişi) gibi yıkıcı teknolojilerin benimsenmesini engelleyebilmektedir.

Kelly (2019) blokzincir teknolojisinin mevcut durumunu 1994 yılındaki internet veya 2005 yılındaki sosyal medyanın durumuna benzeterek herkesin bazı büyük ve önemli etkilerinin olacağını bildiğini, ancak bunların nasıl olacağını kesin olarak kimsenin bilmediğini öne sürerek teknolojinin üst yöneticiler ve yönetim kurulları için bazı sorunlara yol açma potansiyeli taşıdığını bildirmektedir. Bu belirsizlik koşullarında, üst yöneticilerin en büyük endişelerinden biri inovasyon ve yeni teknolojileri kucaklamakta yetersiz kalmaktır.

Blokzincir teknolojinin ilk ve en yaygın uygulama alanı olan kripto paralar devletlerin en fazla endişe duyduğu konudur. Houben ve Snyers (2020) tarafından Avrupa Birliği için hazırlanan raporda özellikle yasal düzenlemeler bağlamındaki bu endişeler küresel sabitlenmiş kripto paraların (stablecions) finansal istikrarı ve para politikalarını tehdit etmesi, kara paranın aklanması ve terör faaliyetlerinin finansmanı, tüketici ve yatırımcı haklarının ihlali, siber güvenlik, finans kuruluşlarının fonlarına güvenilir bir katkı sunmaması, mevcut Kara Para Aklamayı Önleme Yönergesi (AMLD5) mevzuatının illegal faaliyetleri önlemede yetersiz kalması, mevcut yasal düzenlemelerin kripto varlıklara nasıl uygulanacağının belirlenememesi olarak sıralanmaktadır.

Blokzincir teknolojisinin en önemli ve sık karşılaşılan uygulaması olan kripto paralarla ilgili en önemli riskler kripto paraların yolsuzluk, terör faaliyeterinin finansmanı ve kara paranın aklanması gibi kriminal faaliyetlerde kullanılması ve kripto paralara yatırım yapmak isteyen tüketicilerin korunması için gerekli düzenlemelerin henüz yetersiz olmasıdır (Schep, Godlieb ve Röell, 2019). Kara para aklama konusundaki endişe kaynaklarından bir diğeri de merkeziyetsiz finans (DeFi) kavramının ortaya çıkmasıdır. Farklı finansal araçların izin gerektirmeyen ve merkezi olmayan bir versiyonu olan DeFi ile varlık alışverişi, borç alma ve verme ve sanal varlıkların yaratılması gibi işlemler gerçekleştirilebilmektedir. Örneğin, Uniswap adlı herkese açık, açık kaynak kodlu ve Ethereum blokzincir platformu üzerinde çalışan uygulama ile herhangi bir müşteri kimlik bilgisi gerekmeksizin finansal işlemler Kara Paranın Aklanmasının Önlenmesi yasalarına aykırı biçimde gerçekleştirilebilmektedir. TRT World web sitesinde yer verilen Diwakar'ın (2022) makalesine göre 2022 yılı başı itibariyle DeFi uygulamalarında kilitlenmiş olan para tutarı yaklaşık 189 milyar $'dır.

LeMahieu (2018) blokzincir ağlarında karşılaşılabilecek bazı saldırı tipleri arasında sürekli işlem paketleri yollama (transaction flooding), Sybil saldırısı, penny-spend saldırısı, %51 saldırısını saymaktadır. Kötü niyetli bir kullanıcının ağ kapasitesini doldurmak amacıyla kendi kontrolü altındaki hesaplardan birçok gereksiz ancak geçerli işlem göndermesi biçimindeki saldırı "transaction flooding" olarak adlandırılmaktadır. İş İspatı mutabakat mekanizmasında bu saldırıya karşı önlem alınmıştır. Çok sayıda sahte kimlikle bir ağı kontrol etme teşebbüsü olarak tanımlanan Sybil saldırısı blokzincir ağları için de söz konusu olan bir saldırı tipidir. Hisse İspatı gibi oy kullanma hakkının sahip olunan varlıkla ilişkilendirildiği mutabakat protokollerini kullanan ağlarda bu saldırının sağlayacağı bir kazanç bulunmamaktadır. Penny-spend saldırısı ise bir saldırganın, düğümlerin depolama

kaynaklarını boşa harcamak için çok sayıda hesap tarafından çok küçük miktarlı işlemlerin gerçekleştirilmesidir. İş İspatı mutabakat mekanizmasını kullanan blokzincir ağında, bir kullanıcının ya da birlikte hareket eden kullanıcı grubunun ağdaki işlemci gücününün %50'sinden fazlasına sahip olarak ağın kontrolünü ele geçirmesi %51 saldırısı olarak adlandırılmaktadır. Ağdaki kullanıcı sayısı arttıkça %51 saldırısının gerçekleşme ihtimali azalmaktadır.

Sonuç olarak, blokzincir teknolojisinin zayıf yönleri ve taşıdığı riskler ile maruz olduğu tehditler aşağıdaki biçimde listelenmektedir:

Zayıf yönler:

- Genel tasarımı itibariyle genel veri depolamaya (büyük boyutlu verilere) uygun olmaması
- Yasal riskler taşıması ve düzenleyici çerçevenin olmaması
- Teknolojinin henüz olgunlaşmamış olması
- Ölçeklenebilirlik ve performans kaygıları
- Uygun kullanım durumları ve senaryolarının yetersizliği
- Veri güvenliği gelişmiş şifreleme teknikleri ile ileri düzeyde sağlanmış olmakla birlikte, kullanıcıların kriptografik anahtarları uygun biçimde saklamaları gerekliliği
- Blokzincir ağının genişlemesinin neden olacağı işlem gecikmesi
- Veri depolama gereksiniminden kaynaklanacak ölçeklenebilirlik sorunları
- Mevcut Müşterini Tanı ve Kara Paranın Aklanmasının Önlenmesi düzenlemelerine uyum güçlüğü
- Verilerin değiştirilemez oluşu
- Blokzincir konusundaki olumsuz yargılar ve kötü itibar
- İş İspatı mutabakat modeli ile ilgili sorunlar (yüksek enerji tüketimi)
- Blokzincir üçlü çelişkisi (merkezsizlik, ölçeklenebilirlik ve güvenlik)
- Karmaşıklık ve anlaşılmasının güçlüğü
- Farklı dağıtık kayıt sistemlerinin birlikte çalışamaması
- Büyük platformları yükseltme ya da geliştirme güçlükleri
- Yüksek işlem hacmi gerektiren işlemlerde mevcut merkezi veri tabanı sistemlerinin gerisinde kalması

- Akıllı sözleşmelerin kullanımı gibi bazı durumlarda blokzincir sistemi dışından bazı güvenilir bilgilere erişilme gerekliliği
- Sınırlı miktarda arz edilen kripto para durumlarında, teşvik sisteminin sona ermesi ile sistemin nasıl işleyeceğinin öngörülememesi

Riskler ve Tehditler:

- Mevcut iş süreçlerinin değiştirilmesi konusundaki isteksizlik
- Veri koruma, mahremiyet ve gizlilik düzenlemelerine uyum ve veri koruma yasalarından kaynaklanan potansiyel problemler
- AB Genel Veri Koruma Yasası (GDPR) gibi düzenlemelere uyumsuzluk
- Bilinmeyen fayda/maliyet
- Birden fazla yetki alanına dağılmış olan, yönetişimi güç yapı
- Siber saldırılar (kaba kuvvet saldırıları, DDoS saldırıları, çifte harcama, akıllı sözleşmelerdeki program kodlarını hedef alan saldırılar, sürekli işlem paketleri yollama (transaction flooding), Sybil saldırısı, penny-spend saldırısı, %51 saldırısı)
- Blokzincir ağı tüm dünyaya açık olduğundan gizli bilgilerin ülke dışına çıkarılması
- Endüstri standartlarının henüz olmaması nedeniyle farklı blokzincirlerin birlikte çalışmasında yaşanacak problemler
- Yasal düzenlemelerin teknolojinin hızına yetişememesi
- Yüksek yatırım maliyeti
- Kripto para işlemleri için borsalar ve cüzdan sağlayıcılarına olan gereksinim
- Çok sayıda farklı blokzincir platformunun ortaya çıkması sonucunda ekosistemin dağılması, araştırma, geliştirme ve uygulama alanlarında gereken uzmanlık düzeyine ulaşmak için gerekli bilginin parçalanması
- Merkezi olmayan yönetişim mekanizmaları konusundaki yetersiz deneyim
- Kuantum bilişim alanındaki gelişmelerle birlikte şifreleme konusunda gelecekte çeşitli zafiyetler
- Hesaplara erişim şifresinin unutulması, hatalı işlem gerçekleştirilmesi gibi istenmeyen durumlar ortaya çıktığında bu durumu gidermek için başvurulabilecek bir merci, işlemleri iptal edecek ya da silecek bir mekanizma bulunmaması
- Mutabakat mekanizmasının yanlış seçilmesi ya da uygun biçimde tasarlanmaması sonucunda çatallanma, mutabakat hatası ve merkezileşme sonucunda %51 saldırısı
- Akıllı sözleşmelerdeki kodlama hataları.

2.1.8. Blokzincir ile merkezi veritabanı karşılaştırması

Blokzincir teknolojisi temelinde birbiri arasında güven ilişkisi olmayan bir grup tarafından doğrudan paylaşılan, merkezi bir yöneticisi bulunmayan, kayıt defterine yalnızca veri eklemeye ve eklenen verileri görüntülemeye izin veren yeni bir veri saklama yapısıdır. Blokzincirin bu temel özellikleri bilinen klasik veri tabanlarına zıt bir durum teşkil etmektedir. Blokzincir teknolojisi ile klasik veri tabanlarının karşılaştırılması dört ana başlık altında yapılabilir:

- Yönetim yapısı: Blokzincir teknolojisinde veri tabanlarında olduğu gibi merkezi bir yöneticiye gerek duyulmamaktadır. İşlemler çok sayıda bağımsız düğüm tarafından doğrulanır, bir mutabakat mekanizması düğümlerin birbirleriyle senkronize olmasını sağlar. Geleneksel veri tabanları genel güveni kazanmış, uzun süredir kendilerini ispat etmiştir. Ancak özellikle kritik verileri içeren veri tabanlarının tasarımı, kontrolü ve yönetimi için çok sayıda sürece ve insana gereksinim duyulur. Gereksinim duyulan bu kaynaklar için de önemli miktarda zaman ve para ayırmak gerekmektedir. Blokzincir bu veri tabanlarının yerine akıllı bir kriptografi ile tasarlanmış dağıtık bir veri tabanı sunmaktadır.
- Mahremiyet: Blokzincirdeki her bir düğüm her işlemi birbirlerinden bağımsız olarak işlemekte ve doğrulamaktadır. Düğümler bu işlemi kayıt defterinin mevcut durumunu, işlem tarafından talep edilen değişikliği ve işlemin kaynağını gösteren dijital imzayı tamamen görebilmesi sayesinde yapabilmektedir. Bu şüphesiz çok yeni ve çok zekice kurgulanmış bir sistemdir ancak özellikle finansal uygulamalar için işlemlerin tamamen şeffaf biçimde görülebilir olması bazen istenen bir durum değildir. Geleneksel veri tabanları merkezi yönetimle kullanıcıların yapabilecekleri işlemleri kısıtlayabilmektedir. Blokzincir teknolojisindeki mahremiyeti artırmak için geliştirilmiş olan bazı stratejiler bulunmaktadır. Bunlardan bazıları çok sayıda blokzincir adresi altında işlem yapma, gizli işlem yapma, kriptografik karıştırma algoritmaları ve sıfır bilgi ispatı (zero knowledge proofs) olarak adlandırılan ileri kriptografik teknikler biçimindedir. Ancak, bir blokzincirde daha fazla bilgi tutmak, çok daha ağır bir işlem yükü anlamına gelmektedir.
- Dayanıklılık: Blokzincire dayalı veri tabanlarının bir avantajı da yüksek hata toleransıdır. Ağa dâhil her düğüm her işlemi proses etmekte olup hiçbir düğümün kritik bir rolü yoktur. Benzer biçimde, her düğüm birbirine eşten eşe ağ kapsamında bağlıdır ve böylece eşler arasındaki birçok iletişim hattı kopsa bile işlemler durma noktasına

gelmez. Blokzincir, sistemle bağlantısı kesilen her bir düğümün yeniden bağlantı sağladıktan sonra, kaçırdığı işlemleri yakalamasını garanti eder. Klasik veri tabanları replikasyon işlemi için birçok teknik sunmaktadır. Blokzincir ise bu işlemi yepyeni bir seviyeye taşımıştır. Herhangi bir konfigürasyon işlemi gerekmemekte, düğümler ağa kolaylıkla dahil olup ağdan istedikleri gibi çıkabilmektedirler. Son olarak da harici kullanıcılar işlemlerini herhangi bir düğüme veya çok sayıda düğüme aynı anda gönderebilmekte ve bu işlemler otomatik olarak ve sorunsuz bir biçimde herkese duyurulmaktadır. Geleneksel veri tabanlarında yüksek erişilebilirlik düzeyi için pahalı bir altyapı, karmaşık bir konfigürasyon ve felaket kurtarma stratejisi gerekmektedir. Dünyanın farklı yerlerinde bulunan örneğin 10 blokzincir düğümüne sahip bir sistemde ise tüm düğümler birbirine bağlıdır. Eşten eşe esasına dayalı biçimde işlemleri paylaşırlar ve mutabakatı sağlamak için blokzinciri kullanırlar. İşlem yapan son kullanıcılar örneğin bu düğümlerden beşine erişebildiğinde bazı hatların devre dışı olması problem teşkil etmez. Bir ya da iki düğümün bir gün boyunca devre dışı olması halinde de yeterli sayıda kopyanın dolaşımda olması nedeniyle kimse bu durumu fark bile etmeyecektir.

- Performans: Blokzincirin merkezi veri tabanlarına göre daima daha yavaş olacağı öngörülmektedir. Bu teknoloji henüz nispeten yenidir ve optimize edilememiştir. Ayrıca bu yavaşlık blokzincirin doğası gereğidir. Bir işlem gerçekleştirilirken blokzincir klasik bir veri tabanı ile aynı işlemleri gerçekleştirmekle birlikte ilave olarak yük getiren üç ekstra işlem yürütür:
  - İmza doğrulama: Her blokzincir işlemi gizli-açık kriptografik şema kullanılarak dijital olarak imzalanmalıdır. Aksi halde işlemlerin kaynağının ispatlanabilmesi mümkün değildir. Bu imzaların yaratılması ve doğrulanması sayısal bakımdan karmaşık bir işlemdir. Merkezi veri tabanında ise bağlantı bir defa kurulduktan sonra tekrar tekrar her işlemde müstakil bir doğrulama işlemine gerek yoktur.
  - Mutabakat mekanizması: Blokzincir gibi dağıtık bir veri tabanında, ağdaki düğümlerin bir mutabakata varmasına ihtiyaç duyulur. Kullanılan mutabakat mekanizmasına bağlı olarak çok sayıda ileri ve geri iletişim kurulması ve çatallanma problemleri ile başa çıkılmasını gerektirir.
  - Fazlalık: Bu problem tek bir düğümün değil blokzincirin gerektirdiği hesaplamaların toplam miktarı ile ilgilidir. Merkezi veri tabanları işlemleri bir defa (veya iki) proses ederken bir blokzincirde işlemler her bir düğüm tarafından ayrı ayrı proses edilmelidir.

Anwar (2018) tarafından yapılmış olan geleneksel veri tabanı ile herkese açık blokzincir çözümlerinin genel bir karşılaştırması Çizelge 2.5'te verilmiştir. Bu karşılaştırmada Bitcoin gibi herkese açık bir blokzincir platformunun özellikleri dikkate alınmıştır. Sonuç olarak, ortak paylaşılan bir veri tabanına ihtiyaç duyulduğunda blokzincir uygun bir çözümdür.

Çizelge 2.5. Blokzincir ile veri tabanının temel farkları (Anwar, 2018)

Blokzincir	Veri tabanı
Merkezi otorite yoktur	Belirli kişiler tarafından yönetilir
Veri ya da varlıkta değişiklik yapmak hemen hemen imkansızdır	Veri veya varlıklar kolaylıkla değiştirilebilir
Tüm veri ve faaliyetler herkesin görmesine açıktır	Tüm veri veya işlemler sadece yetkilendirilmiş kişilerce görülebillir
Aşırı maliyetleri düşürür	Uygulanma süreci maliyetlidir
Yavaştır	Blokzincire göre çok daha hızlıdır
Kullanıcıların birbirlerine güvenmedikleri durumlara uygundur	Karşılıklı güven bulunan ortamlar için uygundur

2.1.9. Blokzincir çeşitleri

Blokzincir genellikle kayıt defterine erişim ve zincirdeki işlemlere ilişkin karar verme yetkisi haklarına göre sınıflandırılır. Temel olarak, kayıt defterine erişim bakımından özel ve açık olarak sınıflandırılan blokzincir, ağ içerisindeki yetkilendirme mekanizmasına göre de izin gerektiren ve gerektirmeyen blokzincir olarak adlandırılır. Özel blokzincirlerde sadece yetkilendirilmiş kullanıcılar blokzincir kayıtlarını görebilir. Blokların geçerliliğinin onaylanması ve işlemlerin gerçekleştirilmesi için yetkilendirme gerektiren blokzincirler ise izin gerektiren blokzincirler olarak adlandırılır.

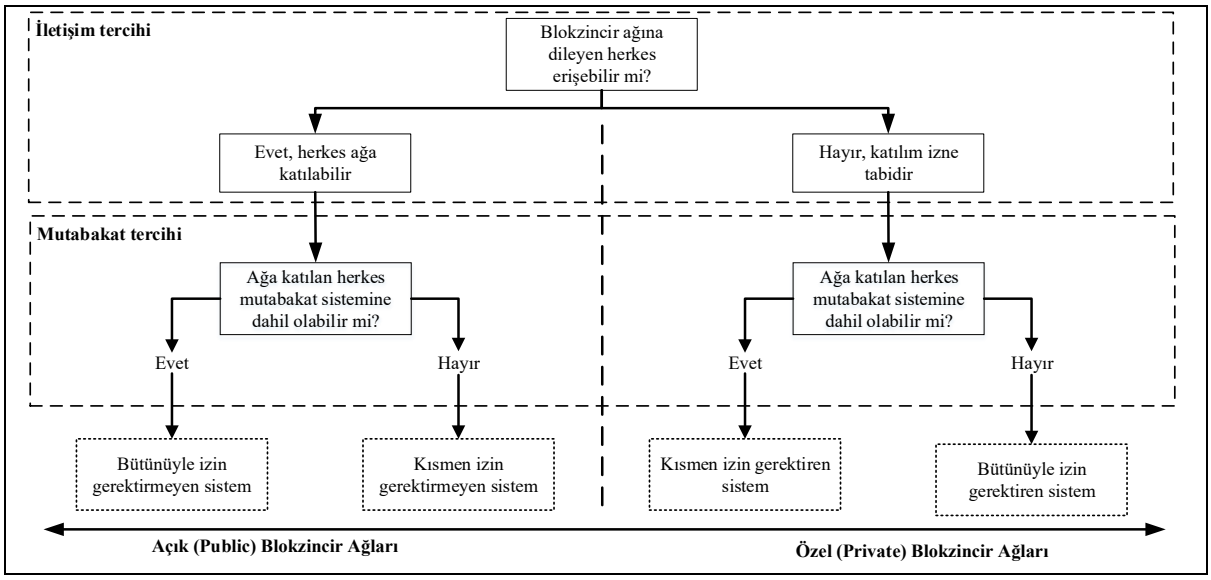
Özel veya açık blokzincirlerden hangisinin kullanılacağı, blokzincir ağının izin gerektiren bir ağ mı yoksa herkesin katılımına müsaade eden anonim bir ağ mı olacağı soruları bir blokzincir çözümü geliştirilirken karar verilmesi gereken ilk konulardan biridir. İzin gerektiren ağlarda üyeler bilinmekte olup ağdaki rollerine göre farklı düzeyde izinlendirme yapılır. Anonim blokzincir ağlarında ise katılımcılar bilinmezler ve erişim tamamen açıktır.

Wall ve Malm (2016) blokzinciri açık, özel, izin gerektirmeyen ve izin gerektiren blokzincirler olarak sınıflandırmaktadır. Açık blokzincir işlem gerçekleştirmek ve veri okumak için hiçbir kısıtlamanın bulunmadığı blokzincirdir. Özel blokzincirde ise yalnızca önceden tanımlanmış olan katılımcılar verilere ve işlemlere doğrudan erişebilirler. İzin

gerektirmeyen blokzincirde ağa katılım için hiçbir kısıtlama yoktur. İzin gerektiren blokzincirde ise sadece yetkilendirilmiş kullanıcılar sisteme erişebilir. İzin mekanizmaları da kendi içerisinde farklılıklar göstermektedir. Örneğin, ağa katılım için herhangi bir izin gerekmezken ağda bazı işlemleri gerçekleştirebilmek için izin gerekebilir.

Kamu uygulamaları için en uygun tip izin gerektiren blokzincirlerdir ve blokzincirin ve kullanıcılarının amacına bağlı olarak Otorite İspatı veya Round Robin modelleri gibi mutabakat modelleri daha uygundur. İzin gerektiren blokzincir, sadece yetkilendirilmiş kullanıcılar yeni işlemleri kaydedebildiğinden ve işlemler herkese açık (şeffaf) olabildiğinden hesap verebilirliği artırmaktadır. Kamu sektöründe devlet kuralları ve kanunlar dikkate alınabilir ve farklı kullanıcı izinleri ve düğümler belirlenebilir. İzin gerektiren ve gerektirmeyen blokzincirlerin farkı internet ile herhangi bir kuruluşun intraneti arasındaki farkla aynı mantıktadır. İnternet herkese açıktır ve herkes internetin inşasına katkıda bulunabilir. Bununla birlikte, intranete erişim için bazı kurallar bulunmaktadır (Berryhill ve diğerleri, 2018).

Usta ve Doğantekin'e göre (2017: 47, 48) blokzincirler temelde açık ve özel olarak ikiye ayrılmakta, blokzincir ağındaki mutabaka sistemine dahil olma yapısı bakımından da izin gerektiren ve izin gerektirmeyen olarak sınıflandırmaktadır. Bu sınıflandırma aşağıda verilmiş olan Şekil 2.7'de gösterilmektedir:



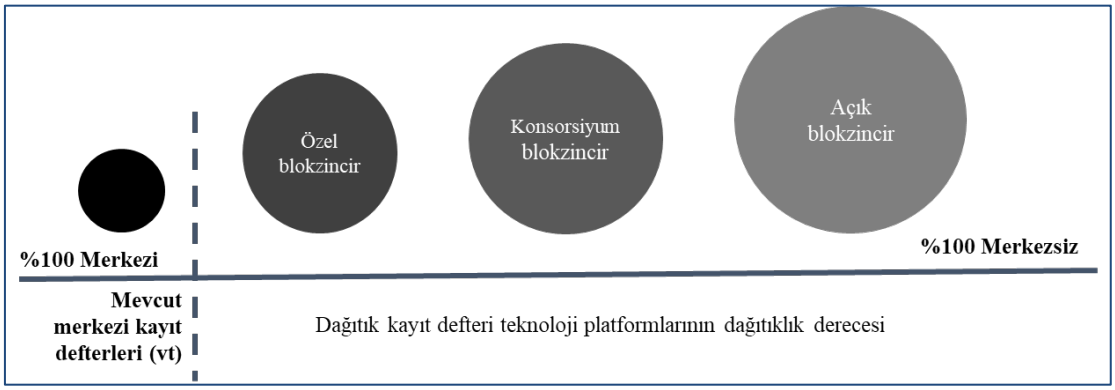
Şekil 2.7. İletişim ve mutabakat tercihine göre blokzincir ağları (Usta ve Doğantekin, 2017: 49)

Açık blokzincirlerin aksine, özel blokzincir ağları aşağıdaki konularda farklı bir yaklaşıma sahip olabilmektedir:

- Okuma izinleri; blokzincirde tutulan verilerin gizlilik derecelerine göre belirlenmiş yetki atamaları istenebilmektedir.
- Blok üretme izinleri; kimlerin madencilik yapabilecekleri ya da işlemleri onaylayabilecekleri sınırlandırılabilmektedir.
- Ağa dâhil olma izinleri; ağa herkesin katılıp katılamayacağı, kimlerin ağa katılıp kimlerin katılamayacağı gibi konularda karar veren merkezi bir otorite ya da mevcut kullanıcılar içerisinde bir mutabakat mekanizması belirlenebilir.
- Kimlik bilgileri; ağa katılanların kimliklerinin tanımlanması zorunluluğu getirilebilir.
- Verilere müdahale; açık blokzincirdeki işlem kayıtlarının değiştirilemezlik özelliğinin aksine, belirli işlemlerin silinebilmesi ya da değiştirilebilmesine imkân veren düzenlemeler getirilebilir.
- Yönetişim; ağın işleyişi, yazılım kodu güncelleme ya da değişiklikleri, çatallanma gibi konularda özel bir karar mekanizması geliştirilebilir.

Blokzincir tipinin açık, özel ya da konsorsiyum biçiminde tasarlanmasında yukarıdaki özellikler dikkate alınır.

Blokzincir ağı özel ve izin gerektiren yapıda tasarlandığında merkezsizlik özelliğini yitirerek merkezi veri tabanlarına yaklaşır. Bitcoin gibi tamamen açık ve izin gerektirmeyen blokzincirler ise %100 merkezi olmayan olarak nitelendirilirler. Aşağıda verilmiş olan Şekil 2.8'de blokzincir çeşitlerinin merkezilik dereceleri gösterilmektedir.



Şekil 2.8. Blokzincir çeşitlerinin merkezilik derecesi

2.1.10. Bizans generalleri problemi ve mükerrer harcama (Double spending)

Bitcoin'in, yayınlandığı tarihe kadar yapılan benzer çalışmalardan en önemli farkı ve üstünlüğü 'Bizans Generalleri Problemi' ya da 'Bizans Hata Toleransı' olarak bilinen duruma getirdiği çözümdür. İlk defa Leslie Lamport ve arkadaşları tarafından 1982 yılında yayınlanmış olan 'Bizans Generalleri Problemi' başlıklı yayında bahsedilen bu durum dağıtık bir sistemdeki bileşenler grubunun güvenilirliğine dayanmaktadır. Savaş halindeki bir ülkenin generallerinin eş zamanlı olarak gerçekleştirilecek bir saldırının planlanmasında birbirlerine gönderdikleri habercilerin kasıtlı ya da manipüle edilmiş olmalarından dolayı yanlış bilgiler verdikleri durumlarda strateji geliştirmek için nasıl iletişim kuracakları ve anlaşacakları fikri üzerine kurulmuş olan bir yapıdır. Özetle, birbirlerine güven duymayan bir grup karar vericinin güvenilir bir biçimde karar vermesi için bir yöntem tasarımıdır.

Bu problemle ortaya konan senaryoya göre her biri Bizans ordusunun bir kısmını komuta eden bir grup general tarafından düşman şehri kuşatılmıştır. Şehre saldırmak için tüm generallerin bir savaş planı üzerinde anlaşmaları gerekmektedir. Generaller arasındaki haberleşme yalnızca haberciler aracılılığıyla gerçekleştirilebilmektedir. Mesajları ileten habercilerin düşman tarafından yakalanması sonucunda mesajın diğer generale ulaşamaması söz konusudur. Durumdaki bir diğer problemli nokta bir ya da daha fazla generalin hain olması ve savaş planını sabote etme olasılığıdır. Bu amaçla bu hain generaller yanlış mesajlar gönderebilir, mesajları manipüle edebilir ya da hiç mesaj göndermeyebilirler. Tüm sadık generaller plana göre hareket ederken az sayıdaki hain tarafından planın bozulmasına izin verilmemelidir (Baliga, 2020).

Lamport, Shostak ve Pease'e (1982) göre yanlış bilgi taşıyan üyelerin sayısı toplam sayının üçte birinden daha az olduğunda promlemin çözümü mümkündür ve uygun bir konsensüs sağlanabilir. Tüm katılımcıların içerisinde yanlış bilgi veren katılımcıların oranı mutabakat sağlanıp sağlanamayacağını gösterir.

Bitcoin'de kullanılan mutabakat mekanizması daha önce yapılamayan bir şekilde bu probleme bir çözüm getirmiştir. İş İspatı olarak adlandırılan yapı ile işlemlerin onayı için Bitcoin ağı içinde mutabakat aranır ve mutabakat sağlanması halinde işlemler gerçekleşir (Nomura Research Institute, 2016).

2.1.11. Mutabakat Mekanizmaları

Dağıtık mutabakat algoritmaları, merkezi olmayan karar vermenin zor ya da imkânsız olduğu durumlarda, ağa bağlı sistemlerin gerekli bir durum ya da fikir üzerinde anlaşmalarını sağlar. Mutabakat, dağıtık bir sistemin tek bir varlık olarak çalışmasını sağlar.

Geleneksel veri depolama sistemlerinde kayıt tutma işlemi genellikle devlet kuruluşları, bankalar, e-posta hizmet sağlayıcısı gibi üçüncü taraflarca gerçekleştirilir. Yönetiminin kolay olmasının yanında merkezi kuruluşlarca tutulan bu kayıtlar tek nokta hatasına açıktır. Ayrıca bu sistemler saldırıya uğradığında veriler çalınabilmekte, değiştirilebilmekte ve silinebilmektedir. Blokzincir teknolojisi bu kayıtları ağdaki tüm düğümlerde tutarak bu merkezi kuruluşlara olan gereksinimi ortadan kaldırır. Blokzincirinin en önemli özelliklerinden biri blok doğrulanıp kaydedilmeden önce düğümlerin çoğunluğu tarafından blok içindeki işlemlerin gözden geçirilerek onaylanması gerekliliğidir. Mutabakat mekanizmaları işte bu onay işlevini yerine getirir. Mutabakat mekanizması, geleneksel sistemlerdeki aracıları ortadan kaldıran özelliktir. Farklı durumlara göre geliştirilmiş farklı mutabakat modelleri bulunmaktadır.

Dağıtık sistemlerdeki geleneksel mutabakat yaklaşımları temelde hata durdurma arızaları için tedbir sağlayan sistemlere karşılık hata toleransı oluşturmaya odaklanmıştır. Dağıtık veri tabanlarında istemci tarafından üretilen taleplerin sıralanması ve ilgili durum değişikliklerinin yapılmasının sağlanması için Paxos (Lamport, Paxos Made Simple, 2001), Raft (Ongaro ve Ousterhout, 2014) ve görme damgalı replikasyon (Oki ve Liskov, 1988) metotları kullanılabilmektedir. Bu algoritmalar, hata durdurma arızaları durumunda fiziksel makinelerde replikasyonu yapılan veri yapılarının tutarlılığını ve ilerlemesini garanti eder. Bu ağlarda “f” tolore edilebilir hata durdurma arıza sayısı olmak üzere gerekli düğüm sayısı “2f+1”dir. Bizans hatalarını tolore edebilmek için sisteme eklenen fazladan mesajlaşma katmanı mutabakat protokolünün karmaşıklığını artırır (Baliga, 2020).

Paxos algoritmasının temelinde eski Yunan toplumundaki sinod (meclis) yatmaktadır. Algoritmanın odaklandığı problem, değer üreten bir dizi süreç içerisinden bir tanesinin seçilmesi, eğer değer önerisi yoksa seçim yapılmaması, seçim yapıldıysa seçilen değerin süreç tarafından öğrenilmesidir. Mutabakat için güvenlik gereksinimleri; yalnızca önerilen çözümler içinden seçim yapılması, sadece bir değer seçilmesi ve gerçekten seçilmediği

sürece hiçbir değerin öğrenilmemesidir. Algoritmada önericiler, onaylayıcılar ve öğrenenler olmak üzere üç sınıf yer alır. Bu sınıfların üyeleri birbirleriyle mesajlaşmaktadır ve bu asenkron mesajlaşma Bizanslı hata modeline uygun olmayan mesaj içeriğinin bozulmadığı biçimde gerçekleşmektedir (Lamport, Paxos Made Simple, 2001).

Bir diğer mutabakat algoritması olan Raft Paxos'a eşdeğer bir sonuç üretmektedir ancak yapısı Paxos'tan farklıdır. Bu farklı yapısı Raft'ı Paxos'a göre daha anlaşılır kılar ve uygulama sistemleri kurmak için daha iyi bir temel sağlar. Anlaşılabilirliği artırmak için Raft lider seçimi, kayıtların replikasyonu ve güvenlik gibi mutabakatın temel unsurlarını birbirinden ayırarak dikkate alınması gereken durumların sayısını azaltmak için daha güçlü bir tutarlılık derecesi uygular. Raft algoritmasında mutabakat öncelikle ayrı bir lider seçilerek çoğaltılmış kayıtların yönetim sorumluluğunun bu lidere verilmesi ile başlar. Bu lider, istemcilerden gelen kayıt girişlerini kabul ederek diğer sunuculara bunları dağıtır (Ongaro ve Ousterhout, 2014).

Görme damgalı replikasyon, Oki ve Liskov (1988) tarafından, dağıtık sistemlerde yüksek erişilebilirliği desteklemek için önerilen bir metottur. Bu metotta, yüksek erişilebilirliği sağlamak için dağıtık bir ağda tutulan işlem kayıtlarının güvenli ve etkin biçimde replikasyonu için zaman damgaları ile ilişkili olan, görme damgası adı verilen kayıtlar kullanılmaktadır.

Mutabakat mekanizmasının yanlış seçilmesi blokzinciri işe yaramaz hale getirerek kaydedilen verileri tehlikeye atabilir. Mutabakat mekanizmasının başarısız olması halinde ortaya çıkabilecek bazı sorunlar aşağıdaki biçimdedir (Baliga, 2020):

- Çatallanma: Blokzincir çatalı sistemdeki farklı düğümlerin farklı bloklar üzerinde birleşmesine neden olabilir. Bitcoin'de ağ gecikmelerinden dolayı geçici çatallanmalar olabilse de, protokol tüm düğümlerin sonunda tek bir zincir üzerinde birleşeceği şekilde tasarlanmıştır. Çatallanma blokzincire kaydedilen verilerin tutarsız görünmesine yol açarak uygulamaların öngörülemeyen bir biçimde davranmasına yol açabilir.
- Mutabakat hatası: Bazı mutabakat algoritmaları mutabakata ulaşma garantisi vermezler. Örneğin, mutabakat için düğümlerin büyük bölümünün oyunun gerektiği algoritmalarda bu rakama ulaşılamaması mutabakat başarısızlığına sebep olabilir.

- Baskınlık (hâkimiyet): Mutabakat algoritması bir ya da bir grup düğümün milyonlarca kimlik üreterek bunları kontrol edebildiği Sybil saldırılarına karşı dirençli olarak tasarlanmadıysa mutabakat sonuçları manipüle edilebilir. Bu tür bir hâkimiyet hakim grubun işlemleri ve blokları kendi kurallarına göre onaylamasına, hatta kripto paralarla çifte harcama yapabilmelerine izin verir. Hâkimiyet İş İspatı ağındaki madenci gücünün %51'ini kontrol etmek gibi başka yollarla da elde edilebilir.
- Aldatma: Doğrulayıcı düğümler tek tek ya da birbirleri ile anlaşarak sahte ya da değiştirilmiş işlemleri onaylayarak blokzincirde paralel çatallar oluşturabilir. Mutabakat mekanizması bu saldırılara karşı korunaklı olmalıdır.
- Zayıf performans: Tasarımına bağlı olarak mutabakat mekanizması belirli koşullarda daha fazla zaman gerektirebilir. Mutabakatın uzun sürmesi işlemlerde birikme ve gecikmelere neden olabilir.

Aşağıda en önemli mutabakat modelleri verilmiş olup uygulamada bu modeller otomatik olarak yazılım tarafından gerçekleştirilmekte, manuel bir müdahale gerekmemektedir.

1. İş İspatı (Proof of Work – PoW)

İş İspatı temelinde üretmesi zor (maliyetli ve zaman alıcı), başkaları için doğrulaması kolay ve belirli, önceden tanımlanmış koşulları karşılayan bir veri parçasıdır. İş İspatı geçerli bir çözüm üretmeden önce ortalama olarak çok sayıda deneme ve yanılma olmasını sağlamak için düşük başarı olasılığı olan, rastgele bir süreç olarak tasarlanmıştır. Bitcoin'de İş İspatının bir varyantı olan Hashcash adlı bir mekanizma kullanılır.

Tüm İş İspatı protokolleri madencilerin kriptografik hash değerlerine dayalı bir bulmaca için çözüm bulunmasını gerektirir. Çözüm, mevcut blok içeriğinin hash değeri ile birlikte hash fonksiyonuna sokulduktan sonra tanımlı bir eşik değerden daha küçük hash değerini verecek olan, nonce adı verilen tek kullanımlık bir değerdir. Bitcoin'de bu işlem için SHA-256 hash fonksiyonu, Ethereum'da Dagger-Hashimoto fonksiyonu, Litecoin ve Dogecoin'de scrypt ve ZCash'te Equihash fonksiyonu kullanılır. Bu kriptografik bulmacanın çözülmesi çok zor, çözümün doğrulanması ise oldukça kolaydır. Bloğun oluşturulma hızı bulmacanın zorluk derecesine bağlıdır. Bitcoin'de bu zorluk derecesi çözümün yaklaşık 10 dakikada bulunmasını sağlayacak biçimde ayarlanır. Sürenin kısa olması çatallanmaya, çatallanma da hem kaynak israfına hem de çifte harcama yapılabilmesine neden olarak güvenlik açığı

oluşturur. Ethereum'da güvenlikten ödün vermeden blok oluşturma süresini kısaltan GHOST adlı bir protokol kullanılır (Dinh ve diğerleri, 2018).

İş İspatı ile anlık işlemler gerçekleştirmek olanaksızdır. İşlemlerin onaylanarak gerçekleşmesi uzun vakit alır. Bu mutabakat mekanizmasının gerektirdiği enerji tüketimi yüksektir (Wall ve Malm, 2016).

İş İspatı, izin gerektirmeyen kayıt defterleri için tasarlanmıştır. Herkesin kayıt defterine veri ekleyebilmesi mümkündür ve herkesteki kayıt defteri özdeştir. Ağa herkes katılabileceğinden dolayı kullanıcılar arasında ortak bir güvensizlik söz konusudur. İş İspatı modeli her kullanıcının kabaca bulmacayı çözme olasılıklarının aynı olmasını garanti eder ve böylelikle belli kullanıcıların hangi blokların zincire ekleneceğini kontrol etmesini engeller.

2. Hisse İspatı (Proof of Stake – PoS)

Madencilerin zincire blok eklemek için karmaşık kriptografik problemleri çözdüğü İş İspatının aksine Hisse İspatında sonraki bloğun yaratıcısı deterministik bir yolla, hisse olarak adlandırılan, sahip olunan varlığa dayalı olarak seçilir. Bu hisse genellikle sahip olunan token ya da kripto parayı ifade etmektedir. Blokzincirde merkezi olmayan kontrolün temeli, ağın bloklar oluşturma hakkının düğümler arasında adil bir şekilde dağıtılmasıdır. Blokları oluşturan kişi tamamen token ya da kripto para bulundurmaya dayalı olarak seçilirse, ağdaki en zengin üye asimetrik bir avantaja sahip olacak ve bu da istenmeyen merkezileştirmeyle sonuçlanacaktır. Bu zorluğun üstesinden gelmek amacıyla, düğüm seçimi için birkaç yöntem önerilmiştir (Wall ve Malm, 2016):

- İlk yaklaşım, hissenin büyüklüğü ile birlikte en düşük hash değerini aramaya dayanır. Bu, bir sonraki blok oluşturucunun seçilmesinde bir dereceye kadar rastgelelik sağlar. Dahası, tüm katılımcıların tüm üyelerin hisselerini bildiği açık blokzincirlerde, her düğüm hangi düğümün bir sonraki bloğu makul bir olasılıkla oluşturma/değiştirme hakkına sahip olacağını tahmin edebilir.
- Diğer yaklaşım sahip olunan hisse ile bunların elde tutulma süresinin bir kombinasyonunun kullanılmasıdır. Daha eski ve daha büyük hisse kümelerinin sonraki

bloğu yaratma olasılığı daha yüksektir. Hisse kullanıldıktan sonra sahiplik süresi sıfırlanır.

Hisse İspatında kriptolojik bulmacanın zorluğu madencinin sahip olduğu hisse ile ters orantılı olacak şekilde değiştirilmektedir. Hisse, madencinin ağı sağlıklı biçimde tutmak için taahhüt ettiği, belirli bir bakiyeye sahip kilitli bir hesaptır (Dinh ve diğerleri, 2018).

Hisse İspatı mekanizması daha fazla hisse sahibi (yani; platformda kullanıcının sahip olduğu kripto paranın miktarı) olan kullanıcıların zincire yeni bloklar ekleme konusunda önceliğe sahip olacak kullanıcılar konusunda karar vermede daha etkin olması mantığına dayanmaktadır. Temel felsefe platformda en fazla hissesi olanların platformun başarılı olması için daha fazla istekli olacakları ve platforma en faydalı olacak kararları verecekleri öngörüsüne dayanmaktadır. Hissenin teminat olarak tutulduğu sistemlerde, kötü niyetli işlemleri yaratan hisse sahiplerinin işlemleri iptal edilerek teminata el konulur. Böylelikle sistem kötü niyetli davranışlara karşı koruma sağlar. Hisse ispatının sınırlılığı "tehlikede olan hiçbir şey olmaması" (nothing at stake) problemi olarak adlandırılan durumdur. Mutabakat sağlanamaması ya da blok üretenlerin birden fazla blokzincir tarihçesi için oy kullanmaları halinde kaybedecekleri bir şey yoktur. Birçok zincir üzerinde çalışmanın İş İspatında olduğu gibi bir maliyeti olmadığından bu problem istismar edilerek çifte harcama yapılabilir.

Baliga (2020) Ethereum platformunun kullandığı Casper adlı PoS algoritmasının en gelişmiş Hisse İspatı algoritması olduğunu öne sürmektedir. Birçok kavram ispatı yapılmasına karşın hala test aşamasına olan Ethereum PoS algoritması Serenity versiyonu ile birlikte kullanılacaktır.

Hisse İspatını pratikte uygulamanın birçok yolu bulunmaktadır. Bazı metotlar platformdaki kripto parasının düzeyine göre rastgele seçim, oylama ve daha yeni olan paranın öncelikli olduğu "coin aging" – coin yaşlandırmayı içermektedir. Coin yaşlandırmada, kullanıcı bir blok yarattığında sahip olduğu kripto paranın yaşı "0" olarak sıfırlanır ve böylelikle bazı kullanıcıların sürekli karar verici olarak güçlü olması engellenmiş olur. İş İspatı gibi, bu mutabakat modeli de karşılıklı güvensizliğin yüksek olduğu ortamlar için iyi tasarlanmıştır. İş İspatından farklı olarak yoğun işlemci kaynağı kullanımını gerektirmez.

3. Yetki İspatı (Proof of Authority – PoA)

Bu modelde "onaylayıcılar" olarak adlandırılan yetkilendirilmiş kullanıcılara blokzincire yeni bloklar doğrulama ve yayınlama kabiliyeti sağlanır. İş İspatı ve Hisse İspatı modellerinden farklı olarak kullanıcının kimliği bilinmeli ve doğrulanmalıdır. Bu doğrulama adımı kritiktir çünkü zincire yeni blok eklemek için kullanıcının yetkisini doğrulamanın tek yolu bu kimliktir. İş İspatı ile karşılaştırıldığında, Yetki İspatı yeni blokların işlenmesi için uzun ve kaynak harcamayı gerektiren işlemler gerektirmediğinden çok daha hızlıdır. Hem izin gerektiren hem de izin gerektirmeyen kayıt defterlerinde kullanılabilir.

Bu mutabakat modeli veritabanı yönetim mantığı ile çok benzerdir. Blokzincir teknolojisi ile ilgili kamu uygulamaları için en uygun mutabakat biçimlerinden biridir.

4. Round Robin

Kullanıcılar arasında belirli bir düzeyde güven mevcut olduğunda, örneğin bilinen kullanıcılardan oluşan izin gerektiren bir ağda, veriye müdahale edilmesi ya da verinin tahrip edilmesi kaygıları daha azdır. Böyle sistemlerde, kullanıcıların blok yayınlamak için dönüşümlü olarak ya da rastgele seçildiği Round Robin yaklaşımı uygun olabilir.

Diğer modellerden farklı olarak Round Robin izin gerektirmeyen ağlarda kullanılamaz. İzin gerektiren kayıt defterleri ile Round Robin'in birlikte kullanımı kamu uygulamaları için en iyi seçenektir. Böyle bir yapıda bir blokzinciri içerisindeki işlemleri görme yetkisi herkese verilirken yeni işlemler ve bloklar yaratma yetkisi sadece yetkilendirilmiş bazı kullanıcılara verilebilir (Berryhill ve diğerleri, 2018).

5. Bizanslı Hata Toleransı (Byzantine Fault Tolarent)

Bizanslı hata toleransı ağın çökme, istikrarsız bağlantı ya da sisteme yapılan saldırılar nedeniyle güvenilir olmadığı durumlarda, blokzincirde mutabakatın sağlanması, durumun yinelenmesi ve işlemlerin yayınlanması gibi konularda kullanılmaktadır. En iyi bilinen ve ve yaygın türleri Pratik Bizanslı Hata Toleransı (PBFT) ve varyantı olan SIEVE'dir. Bu algoritmaların kullanılması sayesinde kayıt defterinin tüm kopyalarındaki işlem sıraları tutarlı hale getirilebilmektedir. Dinh, ve diğerleri (2018) İş İspatında zincire eklenen bloğun,

kendisini takip eden belirli sayıda diğer bloklar tarafından takip edilerek zincir uzatılana kadar onaylanmamasından kaynaklanan nihai olma probleminden bahsederek bu mutabakat mekanizmasında bloğun varlığının olasılıksal, buna karşılık PBFT protokolünün ise aksine deterministik olduğunu belirtmektedir.

Bizanslı Hata Toleransı mutabakat mekanizmasının türleri aşağıdaki biçimdedir:

- PBFT: Castro ve Liskov (2002) tarafından önerilen PBFT, Bizanslı hatasının bulunduğu durumlarda mutabakata varmak için kullanılır. PBFT yinelenen durum makinası kavramını ve tutarlı durum değişiklikleri için eşler arasında bir oylama mekanizmasını kullanır. Diğer mevcut çözümlerle karşılaştırıldığında, kayıt defteri kopyaları ve istemciler arasında alınıp verilen mesajların imzalanması ve şifrelenmesi süreci ile bu mesajların boyutu ve sayısının azaltılması bakımlarından daha pratiktir. Bu algoritma ile performansa düşük bir yük getirilerek, 3f+1 replika ile f Bizanslı hatası tolore edilir. Bunun anlamı, f adet kötü niyetli aktörün bulunduğu ağda bu aktörlerin hatalarının tolre edilmesi için toplam sayının üçte ikisinden fazlası dürüst olmalıdır. Uygulamada ise bu algoritma replika sayısı arttıkça mesajlaşma yükünün çok artması nedeniyle 20 replikaya kadar ölçeklenebilmektedir.

  Karmaşık matematiksel hesaplamalar ve enerji tüketimi gerektirmeyen bir mutabakat mekanizmasıdır. İşlem kesinliği özelliğine sahiptir. Yani, İş İspatının aksine işlemler nihai hale getirildikten ve üzerinde anlaşıldıktan sonra birden fazla teyit gerektirmemektedir. Dağıtık ağdaki düğüm sayısının az olması halinde etkindir. Düğümler arasında yüksek düzeyde iletişim gerektirir. Bu nedenle, düğüm sayısı arttıkça iletişim yükü üstel olarak artar. PBFT ayrıca Sybil saldırılarına açıktır. Ağdaki düğüm sayısının artması Sybil saldırılarını güçleştirmekle birlikte artan sayı ile ölçeklenebilirlik sorunu ortaya çıkmaktadır. Bu nedenle diğer mekanizmalarla kombinasyon halinde kullanılır. PBFT'nin kalite ve performansını artırmak için birçok farklı varyasyonu bulunmaktadır.

- SIEVE: Dağıtık bir ağda, farklı replikalar tarafından çalıştırılması sonucunda, akıllı sözleşmelerin deterministik olmaması farklı çıktılar üretilebilir. Genellikle determisintik olan işlemler SIEVE tarafından yürütüldüğünde de bazen farklı çıktılar meydana gelebilir. Bu protokol akıllı sözleşmeyi bir kara kutu olarak ele alır, tüm işlemleri

spekülatif olarak yürütür ve ardından çıktıları replikalar arasında karşılaştırır. Az sayıda kopya arasında küçük bir farklılık tespit edilirse farklı olan değerler filtrelenir. Eğer fark birçok işlemde meydana gelirse işlemin kendisi filtrelenir.

- Çapraz-Hata Toleransı (XFT): Bizanslı Hata Toleransı protokolleri risk altındaki düğümlerin ve tüm ağın mesaj dağıtımını kontrol etme becerisine sahip güçlü bir düşman olduğunu varsayar. Bu varsayım bu protokollerde karmaşıklığa neden olarak etkinliğini azaltır. XFT yaklaşımı bunun yerine düşmanın düğümlerin çoğunu kontrol edemeyeceğini ve aynı zamanda istediği zaman ağ bölümleri oluşturamayacağını varsayar. Bu basitleştirilmiş model düğümlerin kötü niyetli davranmak için finansal teşviklere sahip olabileceği, ancak düğümler arasındaki iletişimi tehlikeye atacak veya rastgele ağ bölümleri oluşturacak araç ve yeteneklerden yoksun olduğu blokzincirde özellikle ilgi çekicidir. XFT replikaların çoğunun doğru olduğu ve birbirleriyle eşzamanlı olarak iletişim kurabildiği sürece doğru hizmet sağlar.

6. Geçen Zamanın İspatı (Proof of Elapsed Time – PoET)

PoET lider seçimi kavramına dayanır ve ağdaki tüm madencilerin Güvenilir Çalıştırma Ortamı (Trusted Execution Environment - TEE) çalıştırmasını gerektirir. Her madenci TEE üzerinde çalışan koddan bir bekleme zamanı değeri talep eder. En kısa bekleme süresine sahip olan madenci lider olmak için piyangoyu kazanmış olur. TEE içerisindeki fonksiyonlar, harici yazılımlarca tahrif edilerek çalıştırılmaya karşı korumalıdır. Lider olduğunu iddia ederek bir blok yaratan madenci, diğer düğümlerin doğrulayabilecekleri TEE içerisinde üretilmiş ispatı da gösterebilir. Örneğin, liderin en kısa bekleme süresine sahip olduğunu kanıtlaması ve bir sonraki bloğu kazmadan önce protokol tarafından belirlenen süre kadar beklemesi gerekir. Bekleme sürelerinin üretilmesindeki rastgelelik liderlik seçiminin tüm onaylayıcı düğümler ya da madenciler arasında rastgele dağıtılmasını sağlar. Temel dezavantajı özel bir donanıma bağlı olmasıdır.

Intel tarafından geliştirilen ve daha sonra açık kaynak kodlu olarak kullanıma sunulan IntelLedger ya da Intel Sawtooth adlı blokzincir platformunda PoET kullanılmaktadır. Proje hâlihazırda, daha fazla geliştirilmesi için Linux Vakfı Hyperledger projesine devredilmiştir.

7. Federe Bizans Anlaşması (Federated Byzantine Agreement)

Bu protokol ailesi, mutabakat protokollerinin BFT gibi geleneksel güvenlik varsayımlarından ayrılarak bu varsayımları daha esnek hale getirir. Örneğin, protokolün tolerans gösterdiği düğüm gizli anlaşmaları hakkında genel varsayımlarda bulunmak yerine ağdaki düğümler güvendikleri düğümlerin listesini önceden bildirirler. Bu tür mutabakat Ripple ve Stellar gibi tanınmış iki blokzincir platformu tarafından kullanılmaktadır.

Ripple mutabakat protokolü algoritmasında ağdaki her düğüm kendisine karşı işbirliği yapmayacağına güvenilen diğer düğümlerin kimliklerinden oluşan benzersiz bir düğüm listesi (Unique Node Lists - UNL) tutar. Ağdaki mutabakat her turda tüm düğümlerin aday küme adı verilen bir veri yapısında işlemleri topladığı ve bunu UNL'sindeki diğer düğümlere yayınladığı birden fazla turda sağlanır. Her düğüm işlemleri doğrular, oylar ve oylarını yayınlar. Her düğümde belirlenmiş olan adaylar biriken oylara göre rafine edilir ve en çok oy alan işlemler bir sonraki tura geçer. Bir aday küme UNL'deki tüm düğümlerden %80 oy alırsa aday küme geçerli bir blok haline gelir ve her düğüm tarafından blokzincire eklenir. Bir sonraki mutabakat turu daha önceki mutabakat turunda doğrulanmamış bekleyen işlemler ve yeni işlemlerle başlatılır (Baliga, 2020). Her bir alt ağ mutabakat sağladığında tüm ağ da mutabakatı sağlamış olur.

Stellar mutabakat protokolü de Ripple'a benzer. Stellar'da sadece doğrulayıcı düğümler mutabakat protokolüne katılır ve Ripple UNL'ye benzer biçimde her doğrulayıcı yeterli çoğunluk veya çekirdek dilimi (quorum slice) adı verilen kendi kümesini çıkarır. Yeterli çoğunluk, mutabakata varmak için yeterli olan düğümler kümesidir ve yeterli çoğunluk dilimi de belirli bir düğümü mutabakat konusunda ikna edebilen bir alt kümedir. Bir düğüm, ikna edici kümesindeki eşik değer kadar düğüm tarafından onaylandığında kayıt defteri için bu işlemi kabul eder (Baliga, 2020). Açık katılıma izin vermek için Stellar tek bir düğümün birden fazla yeterli çoğunluk diliminde görülebileceği fikrinden yararlanarak düğümlerin kendi dilimi içerisinden bir düğüm kümesi seçmesine izin verir.

8. Atama Kanıtı (Proof of Assignment - PoAs)

Atama Kanıtı, öncüllerine kıyasla daha az güç gerektiren ve nispeten düşük kaliteli donanım üzerinde çalışabilen bir kriptografik fikir birliği mekanizmasıdır. Bu çalışma mekanizması

temel düzeyde ve sınırlı kapasitedeki madencilik işlevlerine sahip Nesnelerin İnterneti (IoT) uygulamalarında kullanım için uygundur. Nesnelerin İnternetine bağlı cihazların durumlarını koordine etmek üzere optimize edilmiş olan Atama Kanıtı mutabakat modelinde her IoT cihazının mikro madencilik adı verilen basit ama çok önemli kriptografik görevleri gerçekleştirmeleri gerekir.

9. Yakma Kanıtı (Proof of Burn – PoB)

Bu mutabakat mekanizmasında işlem doğrulayıcılar pahalı donanımlara yatırım yapmak yerine kripto para ya da jetonlarını geri alınamayacak bir adrese göndererek yakarlar. Bu kripto varlıkların ulaşılamaz bir adrese (eater address) işlenmesi ile doğrulayıcılar rastgele seçim sürecine dayalı olarak sistemde madencilik yapma ayrıcalığını kazanırlar. Kripto varlıkların yakılması kısa vadeli kayıplar karşılığında uzun vadeli taahhüt anlamına gelir. Tasarıma bağlı olarak, yakılan para blokzincir uygulamasının kendine ait yerel para birimi olabileceği gibi Bitcoin gibi alternatif bir zincire ait bir para da olabilir. Yakılan para ne kadar fazla ise bir sonraki bloğu çıkarmak için seçilme şansı da o kadar fazladır. İş İspatına bir alternatif olmakla birlikte, kaynakların boşa harcandığı bir mekanizmadır.

Kripto varlıklarını yakarak ödül kazanan doğrulayıcılar uzun vadeli yatırımcı konumunda olduklarından istikrarı artıran bir mutabakat biçimidir.

10. Kapasite Kanıtı (Proof of Capacity - PoC)

Bu mutabakat tipinde doğrulayıcıların pahalı donanımlara yatırım yapmak ya da kripto varlık yakmak yerine sabit disk alanlarına yatırım yapmaları beklenir. Doğrulayıcılar ne kadar fazla sabit disk alanına sahipse bir sonraki bloğu kazmak ve blok ödülünü kazanmak için seçilme şansı o kadar artar. İş İspatı ve Hisse İspatı sistemlerine kıyasla daha verimlidir.

Kapasite Kanıtı, blok başlığındaki sayıları tekrar tekrar değiştirmek ve bir İş İspatı sisteminde olduğu gibi çözüm değeri için sürekli hash değeri hesaplamak yerine, madencilik faaliyeti başlamadan önce madencilik cihazının sabit diskinde olası çözümlerin bir listesini saklayarak çalışır. Sabit disk ne kadar büyükse, sabit diskte o kadar fazla olası çözüm değeri depolanabilir, bir madencinin listesinden gerekli hash değerini eşleştirme şansı o kadar artar ve bu da madencilik ödülünü kazanma şansını artırır.

11. Etkinlik Kanıtı (Proof of Activity)

Etkinlik Kanıtı, yaygın olarak kullanılan İş İspatı ve Hisse İspatı mutabakat mekanizmalarını birleştiren karma bir yaklaşımdır. Etkinlik Kanıtında madencilik süreci, çeşitli madencilerin yeni bir blok bulmak için daha yüksek hesaplama gücüyle birbirlerini geride bırakmaya çalıştıkları standart bir İş İspatı süreci olarak başlar. Yeni bir blok bulunduğunda yani madencilik yapıldığında, sistem, yalnızca bir başlık ve madencinin ödül adresini içeren yeni bulunan blokla Hisse İspatına geçer. Başlık ayrıntılarına bağlı olarak, yeni bloğu doğrulaması veya imzalaması gereken blokzincir ağından yeni bir rastgele onaylayıcı grubu seçilir. Bir doğrulayıcının sahip olduğu kripto paralar ne kadar fazlaysa, imzalayan olarak seçilme şansı o kadar artar. Tüm doğrulayıcılar yeni bulunan bloğu imzaladıktan sonra blok blokzincir ağına eklenir ve işlemler üzerine kaydedilmeye başlar. Seçilen doğrulayıcılardan bazılarının bloğu tamamlamak için imzalayamaması durumunda, işlem kripto varlık miktarına bağlı olarak rastgele seçilen yeni bir onaylayıcı seti ile bir sonraki kazanan bloğa geçer ve süreç, kazanan blok parayı alana kadar devam eder. Madencilik ücret ve ödülleri, blokta imza atmak için kendi rollerine katkıda bulunan madenci ve çeşitli onaylayıcılar arasında paylaştırılır.

12. Önem Kanıtı (Proof of Importance – PoI)

Önem kanıtı, hangi kullanıcıların blokzincire yeni bir veri bloğu eklemek ve ilgili ödemeyi almak için gerekli hesaplamaları yapmaya uygun olduğunu belirlemek için kullanılan bir sistemdir. Bu mutabakat mekanizmasında madenciler gerçekleştirdikleri ilgili kripto para birimindeki işlem sayısına göre önceliklendirilir. Kripto para cüzdanına ne kadar çok işlem yapılırsa, madencilik faaliyetine atanma şansı o kadar yüksek olur. Önem kanıtı sistemleri, madencileri cüzdanlarından yapılan işlemlerin miktarlarına ve boyutlarına göre önceliklendirerek bir kripto para biriminde aktif olarak işlem yapan kullanıcıları ödüllendirmek için tasarlanmıştır.

Bu mutabakat protokolleri dışında örneğin IOTA Tangle adlı kendi mutabakat protokolünü kullanmaktadır. Mevcut mutabakat protokollerinin temelde Paxos'a dayalı klasik protokoller ve Bitcoin'de kullanılan İş İspatı protokolü olarak ikiye ayrıldığı, klasik protokollerinin mesaj karmaşıklığı, kesin üyelik bilgisi ihtiyacı ve güvenlik zafiyeti, İş

İspatının ise madencilik yarışı ve ölçeklenebilirlik sorunlarına sahip olduğu fikrinden hareketle geliştirilmiştir.

2.1.12. Blokzincir platformları

Blokzincir teknolojisi genel özellikleri itibariyle tek bir kavram olarak anlatılmakla birlikte, farklı sorunlara yönelik olarak tasarlanmış, çalışma biçimi, yapısı ve kullanım amacı bakımından farklılıklar gösteren birçok farklı blokzincir tasarımı bulunmaktadır. Bu farklı tasarımlar blokzincir platformları olarak adlandırılmakta olup ilk ve en popüler blokzincir platformu Bitcoin'dir. Blokzincir teknolojisi ile yeni uygulama geliştirilirken genellikle yeni bir blokzincir altyapısı kodlanmaz, mevcut blokzincir platformları kullanılır. Bu nedenle, blokzincir uygulaması geliştirilmeden önce çözüm aranan sorunun ve uygulamanın özelliklerine en uygun platformun seçilmesi çok önemlidir.

Platformların çeşitliliği ve sayısının fazlalığı kullanım amacına en uygununu seçme konusunda güçlük yaratmaktadır. Her bir kullanım amacının kendine has birçok özelliği bulunabileceğinden, platform seçiminde bu özelliklerin dikkate alınması, en kritik olan özelliklerin belirlenerek belirli bir sınıflandırma doğrultusunda seçim alternatiflerinin değerlendirilmesi gerekmektedir. Hayat ve Winkler (2022) platformların ve bu platformlarının özelliklerinin belirlenmesinde literatürün tek başına yeterli olmayacağını öne sürerek G2, Hacker Noon, DZone, ValueCoders, Gartner, Medium, LeewayHertz, ReadWrite ve TechnoDuet gibi bilgi teknolojisi alanına özgü yayıncılar tarafından yayınlanan teknoloji makalelerini analiz etmiş, blokzincir platformu karşılaştırmaları için olgunluk, blokzincir tipi, programlama dili, fikir birliği protokolleri, akıllı sözleşmeler, ölçeklenebilirlik özelliklerini dikkate almıştır. Benzer biçimde, Nanayakkara, Rodrigo, Perera ve Weerasuriya (2021) ise bu özellikleri belirlemek için açık internetin yeterli olmadığı görüşü ile Capterra, LeewayHertz, G2, Tech Target, HFS gibi tanınmış yayıncılar tarafından yayınlanan farklı açık arama motorları ve araştırma bloglarında bir keşif süreci yürütmüşlerdir. Bu çalışmalar ile İkinci Bölümde detayları verilen blokzincir özellikleri konu başlıkları bir arada değerlendirilerek platformlar değerlendirilirken her biri için teknik özellikler, performansa ilişkin özellikler, güvenlik, kullanım amacı ve niteliksel özellikler olmak üzere ana başlıklar altında değerlendirme kriterleri belirlenmiştir. Bu kriterler şablon olarak her bir platformda kullanılmak üzere Çizelge 2.6'da verilmiştir:

Çizelge 2.6. Blokzincir platformlarının özelliklerinin belirlenmesi için değerlendirme şablonu

Teknik özellikler	
Ağa katılım	Ağa katılım ve ağda işlem gerçekleştirme ve doğrulama için izin ve yetkilendirme gerekip gerekmediğini ifade etmektedir. • İzin gerektiren (1), İzin gerektirmeyen (2), Her iki tipte de konfigüre edilebilir (3)
Blokzincir tipi	Blokzincirin herkese açık ya da özel olmasını ifade etmektedir. • Açık (1), Özel (2), Her iki tipte de konfigüre edilebilir (3)
Hash fonksiyonu	Platformda kullanılan hash fonksiyonlarını ifade etmektedir. Çok sayıda hash fonksiyonu bulunmakla birlikte bunlardan en önemlileri: SHA-256, SHA-512 (Secure Hashing Algorithm), MD (Message Digest – MD2, MD4, MD5, MD6), RIPEMD (RIPEMD, RIPEMD-128, RIPEMD-256 and RIPEMD-160), Keccak-256, X11, Whirlpool (Whirlpool-0, Whirlpool-T, Whirlpool)
Mutabakat mekanizması	Platformun kullandığı mutabakat mekanizmasını ifade etmektedir. Bölüm 2.1.11'de en önemli mutabakat mekanizmalarına yer verilmiştir.
Yazılım dili	Platformun geliştirilmesinde kullanılan yazılım dillerini ifade etmektedir.
Yazılım tipi	Açık kaynak kodlu, lisanslı vb. yazılım özelliğini ifade etmektedir.
Performans özellikleri	
İşlem hacmi	Belirli bir zaman diliminde (saniye, saat, gün vb.) gerçekleştirilebilen işlem miktarını ifade etmektedir. Elde edilen rakamsal bilgiler doğrultusunda aralıklar belirlenerek "çok düşük" ile "çok yüksek" arasında derecelendirilmektedir. • Çok düşük (1), Düşük (2), Orta (3), Yüksek (4) Çok yüksek (5)
Ağ gecikmesi (blok süresi)	Blokzincirde ağ gecikmesi, bir işlemin bir ağa gönderilmesi ile ağ tarafından ilk kabul onayı arasında geçen süredir. İlk onaydan sonra, ilk onayın ötesinde, daha fazla blok eklendikçe işlem daha kesin hale gelir. Elde edilen rakamsal bilgiler doğrultusunda aralıklar belirlenerek "çok düşük" ile "çok yüksek" arasında derecelendirilmektedir. • Çok düşük (1), Düşük (2), Orta (3), Yüksek (4) Çok yüksek (5)
Ölçeklenebilirlik (side-chain, sharding, plasma-chain, off-chain)	Ölçeklenebilirlik, artan ya da genişleyen iş yükü ya da kapsamına karşılık performans ve verimliliğin korunması demektir. Blokzincirde ölçeklenebilirlik sistemdeki işlem sayısındaki artışın performans ve verimlilikte düşüşe neden olmaması özelliğidir. Örneğin, İş İspatı mutabakat mekanizması kullanan bir sistemin ölçeklenebilirliği blok boyutu ve blok oluşturma zamanı gibi içsel özelliklere bağlıdır. Zaman aralığını azaltmak ya da blok boyutunu artırmak performansı iyileştirir ancak blokzincirde çatallanma riskini artırarak güvenliği azaltabilir. Bu nedenle, ölçeklenebilirlik özelliği değerlendirilirken güvenlik ve merkezsizlik özellikleri ile birlikte değerlendirilmeli, blokzincir üçlü çelişkisi dikkate alınarak ölçeklenebilirlik problemlerine getirilebilecek side-chain, sharding, plasma-chain, off-chain çözümlerinin uygulanabilir olup olmadığı düşünülmelidir. Bu çözümler kısaca aşağıda açıklanmaktadır: Side-chain: Yan zincir, diğer blokzincirlerden gelen verileri doğrulayan ayrı bir blokzincirdir. Ana zincirle paralel olarak çalışır ve ana zincirle yan zincir arasında transfer yapılmasını mümkün kılar. Sharding: Büyük ölçekli veritabanlarında yaygın olarak kullanılan bir tekniktir. Veriler, yüksek eş zamanlılığı sağlamak için yatay olarak her biri bir parça (shard) olarak adlandırılan parçalara bölünür. Blokzincirde tasarımı karmaşık bir işlemdir ve parçaların merkezi kontrolünün kolaylaşması, parçalar arası iletişimin verimi düşürmesi gibi handikaplara sahiptir Off-chain: Zincir dışı teknoloji adından da anlaşılacağı üzere işlemlerin blokzincir üzerinde değil zincir dışında yer aldığı bir çözümdür. Güvenin sağlanması için zincir dışı işlemlerin bir anlaşmazlık arabulucusu olarak hareket eden ana zincir tarafından güvence altına alınması bir başka ifade ile zincir dışı işlemlerin zincir üzerine kaydedilmesi gerekebilir. Plasma-chain: Etherum'da kullanılan, ana blokzincirin altına belirli özel amaçlar için oluşturulmuş çocuk zincirlerin kullanılarak işlemlerin hızlandırıldığı bir çözümdür. • Düşük (1), Orta (2), Yüksek

İşlem hızı	İşlem hızı bir işlem için gerçekleşen talep ile o işlemin sonuçlanması arasında geçen süreyi ifade etmektedir. Elde edilen rakamsal bilgiler doğrultusunda aralıklar belirlenerek "çok düşük" ile "çok yüksek" arasında derecelendirilmektedir. • Çok düşük (1), Düşük (2), Orta (3), Yüksek (4) Çok yüksek (5)
Blokzincir üçlü çelişkisi	Temel üç özellikten (ölçeklenebilirlik, güvenlik, merkezsizlik) hangi ikisinin sağlanıp hangisinden feragat edildiğini ifade etmektedir. • Ölçeklenebilir ve güvenli ama merkezi (1), Ölçeklenebilir ve merkezsiz ama güvensiz (2), Güvenli ve merkezsiz ama ölçeklenebilir değil (3), Ölçeklenebilir, güvenli ve merkezsiz (4)
Güvenliğe ilişkin özellikler	
DoS ve DDoS saldırılarına direnç	Genel olarak internete bağlı sistemlerin sunmuş oldukları hizmetleri aksatmak, kaynaklarını olabildiğince tüketerek çalışmasını yavaşlatmak ya da tamamen durdurmak biçiminde gerçekleştirilen saldırılardır. Blokzincir platformunun bu saldırılara karşı direnci "düşük" ile "yüksek" aralığında derecelendirilmektedir. • Düşük (1), Orta (2), Yüksek (3)
Sybil saldırısına direnç	Sybil saldırısı saldırganın çok sayıda sahte kimlik oluşturarak ağ sisteminin ele geçirilmesi, ya da itibar sisteminin zarara uğratılmasıdır. Blokzincirde bu saldırı ağdaki hesaplama gücünün ya da hash oranının sahte kimliklerle çoğunluğunun ele geçirilmesi ve bu şekilde işlemlerin manipüle edilmesi biçiminde ortaya çıkmaktadır. Blokzincir sisteminin açık, özel olması, kullanılan mutabakat mekanizması gibi özellikler dikkate alınarak bu saldırılara karşı direnç "düşük" ile "yüksek" aralığında derecelendirilmektedir. • Düşük (1), Orta (2), Yüksek (3)
Kuantum bilişim riskine direnç	Kullanılan anahtarların tekrar kullanılması, tek kullanımlık anahtar kullanımı, blok oluşturma zamanı, kullanılan hash ve şifreleme algoritmaları gibi faktörler dikkate alınarak bu saldırılara karşı direnç "düşük" ile "yüksek" aralığında derecelendirilmektedir. • Düşük (1), Orta (2), Yüksek (3)
Mahremiyet ve gizlilik teknolojisi	Platformda kullanılan kriptografik fonksiyonlar, anonimlik tasarımı, işlemlerin açık-gizli anahtarlarla ilişkilendirilmesi gibi özellikler dikkate alınarak mahremiyet ve gizlilik "düşük" ile "yüksek" aralığında derecelendirilmektedir. • Düşük (1), Orta (2), Yüksek (3)
Kullanım amacına ilişkin özellikler	
Uygulama türü	Platformun genel amaçlı mı özel amaçlı mı olduğu, özel amaçlı ile hâlihazırdaki kullanım alanları ifade edilmektedir. Bu kullanım alanları arasında dijital varlık yönetimi, kimlik yönetimi, kripto para işlemleri gibi konular yer almaktadır. • Genel amaçlı (1), Sadece belirli işlemler için (2)
Akıllı sözleşme desteği	Platformun akıllı sözleşme kullanımına uygun olup olmadığı ifade edilmektedir. • Evet (1), Hayır (2)
Akıllı sözleşme dil desteği	Akıllı sözleşmelerin kullanılması için programlama dili sınırlandırmaları varsa bunlara ilişkin bilgiler ifade edilmektedir.
Token kullanımı	Platformda işlem gerçekleştirmek ya da doğrulama-karar mekanizmasında yer almak için ya da farklı amaçlarla token kullanımı gerekip gerekmediği, platformun token üretimi ve kullanımını destekleyip desteklemediği ifade edilmektedir. • Evet (1), Hayır (2)
Niteliksel özellikler	
Olgunluk	Platformun kuruluş tarihi, geliştiricisi, kriptopara desteği varsa pazar payı gibi faktörler dikkate alınarak çok düşük ile çok yüksek arasında ifade edilmektedir. • Çok düşük (1), Düşük (2), Orta (3), Yüksek (4) Çok yüksek (5)
Pazardaki popülarite	Gösterilen ilgi düzeyi, pazar payı verileri kullanılarak, "Trends.google.com", "coinmarketcap.com" gibi kaynaklardan faydalanılarak çok düşük ile çok yüksek arasında ifade edilmektedir. • Çok düşük (1), Düşük (2), Orta (3), Yüksek (4) Çok yüksek (5)
Geliştirici	Platformu geliştiren kişi, grup, kurum ya da kuruluş bilgisini ifade etmektedir.
Güvenilirlik	Olgunluk, popülarite ve geliştirici bilgileri kullanılarak çok düşük ile çok yüksek arasında ifade edilmektedir. • Çok düşük (1), Düşük (2), Orta (3), Yüksek (4) Çok yüksek (5)

Her bir kritere ilişkin değerlendirme ve karşılaştırma yöntemleri ile kriterlerin blokzincir çözümü seçim kararında kullanılmasına ilişkin detaylar Dördüncü Bölümde verilmiştir.

Hâlihazırda, blokzincir uygulamaları geliştirilirken çoğunlukla açık kaynak kodlu olan birçok platform kullanılabilmektedir. Bu platformlar en temelde özel ve açık olmak üzere iki gruba ayrılabilir. Açık blokzincir platformlarına örnek olarak Bitcoin, Ethereum ve Coinbase, özel blokzincir platformlarına örnek olarak da Hyperledger, Ripple, Chain ve Quorum verilebilir. Blokzincir platformlarının bir kısmı özel amaçlar için geliştirilmiş olup Ethereum gibi bir kısmı ise hemen her amaç için kullanılabilecek yapıdadır.

Blokzincir platformlardan Multichain ve Corda Bitcoin'in işleme dayalı veri modelini kullanır. Bitcoin'den farklı olarak, bu platformlar kurumların, varlıkların kontrol edilmesi ve ticareti için kapalı ağlar oluşturmasına izin verir. Dijital varlıkların yaratılması ve yönetimi ile, genellikle akıllı sözleşmeler kullanılarak genel kullanıcı tanımlı uygulamalar desteklenir. Akıllı sözleşmeler konusunda en popüler platform, hesaba dayalı veri modelini kullanan Ethereum'dur. Bu platform, açık ve izin gerektirmeyen uygulamaları destekler. Monax, Hydrachain, Quorum, Dfinity ve Parity Ethereum'dan türetilmiş olan platformlardır (Dinh, ve diğerleri, 2018).

ITU-T (2019b) ile Bano ve diğerleri (2017) bazı blokzincir platformlarının özelliklerini Çizelge 2.7'deki biçimde listelemektedir.

Çizelge 2.7. Bazı blokzincir platformlarının güvenlik ve performans özellikleri

Platform	DoS Direnci	İşlem Hacmi	Ölçeklenebilirlik	Ağ Gecikmesi
ByzCoin	Kısmen	1 000 işlem/sn	X	10-20 sn
Solidus	Kısmen	-	-	-
Algorand	✓	90 işlem/saat	X	40 sn
Hyperledger	✓	110k işlem/sn	X	<1 sn
Tencent TrustSQL	✓	50k işlem/sn	X	20 ms
RSCoin	✓	2k işlem/sn	✓	<1 sn
Elastico	✓	110 saniyede 16 blok	✓	110 sn/16 blok
Omniledger	✓	≈10k işlem/sn	✓	≈1 sn
Chainspace	Kısmen	350 işlem/sn	✓	<1 sn
Ouroboros	✓	257,6 işlem/sn	X	20 sn
Praos	Kısmen	-	-	-
Snow-white	✓	100-150 işlem/sn	✓	?
PermaCoin	✓	-	X	-
SpaceMint	✓	?	X	600 sn
Intel PoET	✓	1 000 işlem/sn	✓	-
REM	✓	!	✓	-

Platform	DoS Direnci	İşlem Hacmi	Ölçeklenebilirlik	Ağ Gecikmesi
Bitcoin	✓	7 işlem/sn	X	600 sn
Bitcoin-NG	Kısmen	7 işlem/sn	X	<1 sn
GHOST	✓	-	X	-
DECOR+HOP	✓	30 işlem/sn	X	60 sn
Spectre	✓	-	X	-

En yaygın biçimde kullanılan blokzincir platformlarına ilişkin genel bilgiler ve yukarıda sıralanmış olan kriterlere (Bkz. Çizelge 2.6) göre özellikleri aşağıda verilmiştir.

- Bitcoin

Yukarıda belirtilmiş olan değerlendirme kriterlerine göre Bitcoin platformunun özellikleri Çizelge 2.8'de verilmiştir.

Çizelge 2.8. Bitcoin platformunun özellikleri

Teknik özellikler	
Ağa katılım	Ağa katılmak için bir yetkilendirme yapılması gerekmemektedir. İsteyen herkes ağa katılıp madencilik yapabilir. • İzin gerektirmeyen (2)
Blokzincir tipi (açık, özel)	Açık (1)
Hash fonksiyonu	SHA-256
Mutabakat mekanizması	İş İspatı (PoW)
Yazılım dili	C++ (%67), Python (%18,8), C (%9,3), M4 (%1,6), Shell (%1,3), Makefile (%1,0), Diğer (%1,0) (Github.com, 2021)
Yazılım tipi	Açık kaynak kodludur. Ücretsiz kullanıma açıktır. Github üzerinde yazılımın tüm geçmişi ve geliştirmeler ile katkı sağlayanlara erişim mümkündür.
Performans özellikleri	
İşlem hacmi[2]	https://www.blockchain.com/charts/n-transactions adresinden sağlanan istatistiklere göre, 2022 yılı Ağustos – Ekim ayları arasındaki üç aylık dönemde gerçekleşen günlük ortalama işlem sayısı yaklaşık 260 bin olup bu rakam **saniyede yaklaşık 3 işleme** denk gelmektedir.
Ağ gecikmesi	Minimum **10 dakika** (Bitcoin blokzincirde blok oluşturma, bir başka deyişle işlemlerin gerçekleşme süresi ortalama 10 dakika olmakla birlikte genel yaklaşım bir bloğun tam olarak geçerli hale geldiğinden emin olmak için 6 blok beklenmesi biçimindedir. Bu da bir saatlik bir zamana tekabül etmektedir)
Ölçeklenebilirlik (side-chain, sharding, plasma-chain, off-chain)	Blok boyutunun sınırlı olması ve İş İspatı mekanizmasındaki zorluk derecesinin blok yaratma zamanını on dakika civarında tutacak biçimde işlemesi nedeniyle Bitcoin blokzincirde ölçeklenebilirlik bir darboğaz yaratmaktadır. Bu nedenle Bitcoin platformunun ölçeklenebilirliği "**düşük**" (1) olarak nitelendirilmektedir.
İşlem hızı	Minimum 10 dakika
Blokzincir üçlü çelişkisi	Bitcoin platformu güvenlik ve merkezsizlik bakımından güçlü, ölçeklenebilirlik bakımından zayıftır. • Güvenli ve merkezsiz ama ölçeklenebilir değil (3)
Güvenliğe ilişkin özellikler	

[2] İşlem hacmi, ağ gecikmesi ve işlem hızı için "çok düşük" ile "çok yüksek" aralığındaki derece tüm platformların birbirleri ile karşılaştırılması sonucunda belirlenmektedir. Bu nedenle platform özellikleri tablolarında yalnızca bu parametrelerin değerlerine yer verilmiştir.

DoS ve DDoS saldırılarına direnç	Bitcoin'de blok boyutu başlangıçta 36 MB'tan daha fazla işlem verisi içermeyecek şekilde belirlenmiş, ancak daha sonra, 2010 yılında, Bitcoin ağını tıkayacak spam işlemler ve dağıtılmış hizmet reddi (DDoS) saldırılarına karşı bir önlem olarak bu boyut 1 MB olarak sınırlandırılmıştır. Bitcoin blokzincirin DDoS saldırılarına karşı direnci "yüksek" olarak nitelendirilmektedir. • Yüksek (3)
Sybil saldırısına direnç	Bitcoin sistemindeki İş İspatı mutabakat mekanizması ağ üyeliği için bir maliyet gerektirdiğinden Sybil saldırısına karşı direnç sağlamakta, bu direç "yüksek" olarak değerlendirilmektedir. • Yüksek (3)
Kuantum bilişim riskine direnç	Bitcoin'de tek kullanımlık açık anahtarlarla işlem yapılması durumunda kuantum bilgisayarlar bir risk taşımakla birlikte, 2010 yılından itibaren kullanılan tek kullanımlık açık anahtarların hash değeri kuantum bilgisayarlara göre dirençlidir. Çünkü bu anahtarların geçerlilik süresi Bitcoin'de işlem doğrulama zamanı olan on dakika ile sınırlıdır. Kuantum bilgisayarların işlem gücüne göre günümüz tahminleri Bitcoin imzalarının şifrelerinin kırılmasının 30 dakikalık bir süre alacağını göstermektedir. Bu nedenle Bitcoin sistemi kuantum bilişim riskine karşı dirençli olarak değerlendirilmektedir. • Yüksek (3)
Mahremiyet ve gizlilik teknolojisi	Kullanıcılar arasındaki işlemlerde gizli ve açık anahtarlarla asimetrik kriptografi, dijital imzalar için eliptik eğri kriptografinin (Elliptic Curve Cryptography - ECC) dijital imza algoritmasını (Elliptic Curve Digital Signing Algorithm), hash fonksiyonu olarak SHA-256 algoritmasını kullanmaktadır. Bitcoin işlemlerinde ECDSA ile üretilen dijital imza daha sonra hash işleminden geçirilerek ikinci bir güvenlik katmanı oluşturmaktadır. • Yüksek (3)
Kullanım amacına ilişkin özellikler	
Uygulama türü	Sadece belirli işlemler için (2) - Kriptopara ve eşler arası ödeme sistemi
Akıllı sözleşme desteği	Karmaşık sözleşmelere uygun olmamakla birlikte çok imzalı hesaplar, zaman kilitleri, çapraz zincirleme transfer işlemleri ve emanet hesapları gibi basit akıllı sözleşmeler kullanılabilmektedir. Akıllı sözleşme uygulaması çok yaygın ve bilindik olmadığından karşılaştırma tablosunda bu özellik "hayır" olarak gösterilmiştir. • Hayır (2)
Akıllı sözleşme dil desteği	Minsc (2019 yılında yayınlanmış olan, miniscript üzerine kurulu script işlemlerini basitleştiren dildir), C++, Golang
Token kullanımı	• Hayır (2)
Niteliksel özellikler	
Olgunluk	İlk blokzincir uygulaması olması, 2009 yılından bu yana duraksamadan çalışıyor olması, kriptopara pazarını domine etmesi gibi nedenlerle olgunluk düzeyi "çok yüksek" olarak değerlendirilmektedir. • Çok yüksek (5)
Pazardaki popülarite	Kriptopara pazarındaki payı %60'ın üzerindedir. En büyük ve en eski kriptopara olarak popülaritesi "çok yüksek" olarak değerlendirilmektedir. • Çok yüksek (5)
Geliştirici	Açık kaynak kodludur, tek bir geliştiricisi ya da kurumsal bir sahibi, yöneticisi bulunmamaktadır. Bitcoincore.org; geliştirme faaliyetleri Github üzerinde çok sayıda (27 Şubat 2021 tarihi itibariyle 338) gönüllü yazılımcı tarafından yürütülmektedir.
Güvenilirlik	Olgunluk, popülarite ve geliştirici özellikleri dikkate alınarak "çok yüksek" olarak değerlendirilmektedir. • Çok yüksek (5)

- Ethereum

2013 yılında yayınladığı tanıtıcı yazı ile Buterin (2013) Ethereum'u genel betik dillerini kullanarak merkezi olmayan uygulamalar geliştirmek için bir araç olarak önermiştir. Ethereum'un resmi gelişimi 2014 yılında Ethereum Switzerland GmbH adlı bir şirket aracılığıyla başlamış, daha sonra katılımcıların Bitcoin ile Ethereum'un tokeni olan Ether satın alabildiği çevrimiçi bir kitlesel fonlama niteliğindeki İlk Dijital Para Arzı (ICO) ile finanse edilen Ethereum Vakfı Kurulmuştur. 2015 yılı Mayıs ayında Olympic adı verilen ilk versiyonu ile kripto dünyasına giren Ethereum'un daha sonra 2015 yılı Temmuz ayında Frontier, 2016 yılı Mart ayında Homestad, 2017 yılı Ekim ayında Metropolis, 2020 yılı Aralık ayında ise Ethereum 2.0 versiyonu olan Serenity yayınlanmıştır.

Ethereum açık kaynak kodlu ve herkese açık blokzincire dayalı dağıtık işlem platformu ve akıllı sözleşmeler ile desteklenen genel bir programlama platformudur. Ethereum'da akıllı sözleşmelerin hazırlanması için Turing complete programlama dili olan, Javascript'in bir alt kümesi Solidity, bunların çalıştırılması için de Ethereum Sanal Makine (EVM) kullanılır. Doğrudan tarayıcı üzerinde akıllı sözleşmeler yaratmak için Ethereum tarafından sağlanan açık kaynak kodlu bir araç olan Remix IDE (Integrated Development Environment) kullanılabilir.

Bitcoin gibi Ethereum da açık ve izin gerektirmeyen bir platformdur ve isteyen herkes bir hesap oluşturmak için Ethereum istemci yazılımını yükleyerek Ethereum ağına dâhil olabilir. Ethereum sisteminde Ether adı verilen kripto para kullanılmaktadır. Ethereum genel amaçlı olarak tasarlanmıştır ve blokzincir kullanılması gereken her uygulamada kullanılabilir.

Ethereum platformunda iki tip hesap bulunmaktadır: Harici Olarak Sahip Olunan Hesaplar (Externally Owned Accounts - EOA) ve Sözleşme Hesapları. Bu platformda bir işlem, EOA tarafından gönderilen mesajı depolayan, dijital olarak imzalanmış veri paketini ifade etmektedir. Bir işlem temel olarak; mesajın alıcısının kimliği ya da adresi, göndericiyi tanımlayan bir imza, gönderici tarafından alıcıya gönderilen ether miktarı, opsiyonel bir veri alanı, işlemin gerçekleşmesi için izin verilen maksimum hesaplama adımını temsil eden STARTGAS değeri, göndericinin hesaplama adımı başına ödediği ücreti temsil eden bir GASPRICE değeri bilgilerini içerir. Ethereum'daki temel hesaplama birimi "gas" olarak

adlandırılır. Her işlem, işlemin kullanabileceği hesaplama adımlarının sayısına STARTGAS alanına bağlı olarak bir sınır koyar. Genel olarak, pahalı hesaplama adımları yüksek miktarda gas gerektirir. Kullanıcılar, GASPRICE alanında belirtildiği biçimde, ağa, örneğin; işlem verilerindeki her bayt için 3 gas gibi, küçük bir işlem ücreti ödemelidir.

Ethereum projesi her biri akıllı sözleşmeler yazmak için programlama dilleri, Ethereum ağıyla etkileşim için son kullanıcı grafik tarayıcıları, ağa katılım için uygun istemciler gibi projenin farklı yönlerine odaklanan 120'den fazla ayrı yazılım havuzundan oluşmaktadır. Ethereum'a uyumlu istemci geliştirmek için çok sayıda yazılım projesi ve koda katkıda bulunan yüzlerce bağımsız geliştirici bulunmaktadır. Ethereum projesinin kodu da tüm geçmişi ile birlikte Bitcoin'inki gibi Github'da ve diğer çevrimiçi depolarda herkese açıktır. Tüm kod gelecekte de aynı biçimde telif korumasız olarak geliştirilmeye ve türevlerinin yaratılmasına devam edebilmesi için LGPL-3 adlı sanal telif müsaadeli lisans ile yayınlanmaktadır (Valkenburgh, 2017). 2022 yılı Ekim ayı itibariyle Github'daki yazılım havuzu sayısı 2 781'e, geliştirici sayısı ise 89'a ulaşmıştır.

Ehtereum platformunda yürütülen akıllı sözleşmelerde Solidity gibi üst düzey bir programlama dili kullanılmaktadır. Solidity ile yazılan sözleşmeler EVM'de derlenir. Programcı Solidity ile fonksiyon setlerini tanımlar ancak EVM fonksiyonları desteklemediğinden derleyici her fonksiyonu fonksiyon adı ve parametrelerine göre benzersiz bir imzaya çevirir. Çalışma zamanında bir fonksiyon çağrıldığında, bu imza sözleşmede girdi olarak kullanılır. İmza belirli bir fonksiyonla eşleşirse ilgili kod yürütülür. Aksi halde geri dönüş fonksiyonuna atlanır. Geri dönüş fonksiyonu keyfi olarak programlanabilen ve adı ve parametresi olmayan özel bir fonksiyondur. Bu fonksiyon aynı zamanda sözleşmeye boş bir imza geçtiğinde de yürütülür. Bu sözleşme yürütme mekanizması geçmişte birçok güvenlik açığına neden olmuştur (Atzei, Bartoletti ve Cimoli, 2017). Belirlenmiş olan değerlendirme kriterlerine göre Ethereum platformunun özellikleri Çizelge 2.9'da verilmiştir.

Çizelge 2.9. Ethereum platformunun özellikleri

Ethereum	
Teknik özellikler	
Ağa katılım	Ağa katılmak için bir yetkilendirme yapılması gerekmemektedir. İsteyen herkes ağa katılıp madencilik yapabilir. • İzin gerektirmeyen (2)

Blokzincir tipi (açık, özel)	Açık (1)
Hash fonksiyonu	Keccak-256
Mutabakat mekanizması	İş İspatı (PoW) kullanılmakta olup Hisse İspatı (PoS) testleri tamamlandıktan sona geçiş yapılacaktır.
Yazılım dili	Ethereum.org adresinde yer alan desteklenen diller arasında Delphi, .NET, Golang, Java, Javascript, Python ve Rust yer almaktadır.
Yazılım tipi	Ethereum projesinin kodu da tüm geçmişi ile birlikte Bitcoin'inki gibi Github'da ve diğer çevrimiçi depolarda herkese açıktır. Tüm kod gelecekte de aynı biçimde telif korumasız olarak geliştirilmeye ve türevlerinin yaratılmasına devam edebilmesi için LGPL-3 adlı sanal telif müsaadeli lisans ile yayınlanmaktadır
Performans özellikleri	
İşlem hacmi	Ethereum ağında saniyede gerçekleştirilen işlem sayısı 10 – 30 aralığındadır. Ethereum.org'da yayınlanan istatistiklere göre, 27 Ekim 2022 tarihinde gerçekleşen günlük işlem sayısı 1,105 milyon olup bu rakam saniyede **13** işleme denk gelmektedir. Gerçekleştirilen işlem sayısına ilişkin darboğaz kullanılan mutabakat mekanizmasından kaynaklanmaktadır. Hisse İspatı mutabakat mekanizmasına geçiş ile bu işlem sayısının büyük oranda artması beklenmektedir.
Ağ gecikmesi	Ethereum ağında blok oluşturma süresi 15 saniye olmakla birlikte işlemlerin tam olarak geçerli olduğundan emin olunması için genel olarak 25 bloğun daha oluşmasının beklenmesi gerekmektedir. Bu da yaklaşık **6 dakikalık** bir süreye denk gelmektedir.
Ölçeklenebilirlik (side-chain, sharding, plasma-chain, off-chain)	Halihazırdaki ölçeklenebilirlik probleminde yönelik olarak tüm Ethereum ağının "parça" – shard adı verilen çok sayıda bölüme ayırarak yönetilmesine dayalı sharding adı verilen bir çözüm geliştirilmektedir. Ölçeklenebilirlik sorununa yönelik olarak geliştirilmekte olan bir diğer çözüm ise plasma-chain'dir. Plasma-chain; Etherum'da kullanılan, ana blokzincirin altına belirli özel amaçlar için oluşturulmuş çocuk zincirlerin kullanılarak işlemlerin hızlandırıldığı bir çözümdür. Mevcut durumda "düşük" olarak değerlendirilmekle birlikte geliştirilmekte olan çözümlerin 2021 yılı içinde devreye alınması beklendiğinden nihai olarak ölçeklenebilirlik "orta" olarak değerlendirilecektir. • Orta (2)
İşlem hızı	Bitcoin'de 10 dakika olan blok onaylanma süresi Ethereum'da 13 – 30 saniye arasında olup 2015 – 2021 yılları arasında gerçekleşen blok onaylanma sürelerinin ortalaması 15 saniyedir. Ethereum.org'a (2022) göre ise blok onaylanma süresi 12 saniyedir.
Blokzincir üçlü çelişkisi	Ethereum platformu güvenlik ve merkezsizlik bakımından güçlü, ölçeklenebilirlik bakımından zayıftır. Ölçeklenebilirlik sorununa yönelik olarak geliştirilmekte olan çözümler ise (sharding ve plasma-chain) merkeziyetsizlik özelliğinden uzaklaşılması anlamına gelmektedir. • Güvenli ve merkezsiz ama ölçeklenebilir değil (3)
Güvenliğe ilişkin özellikler	
DoS ve DDoS saldırılarına direnç	Saldırıların gerçekleştirilmesi bir maliyet getirdiğinden Ethereum platformunun DDoS saldırılarına karşı direnci "yüksek" (3) olarak nitelendirilmektedir.
Sybil saldırısına direnç	Saldırıların gerçekleştirilmesi bir maliyet getirdiğinden Ethereum platformunun Sybil saldırılarına karşı direnci "yüksek" (3) olarak nitelendirilmektedir.
Kuantum bilişim riskine direnç	Ethereum'da kullanılan Lamport imzaları kuantum bilişim riskine karşı dirençlidir. • Yüksek (3)
Mahremiyet ve gizlilik teknolojisi	Ethereum da Bitcoin gibi ECDSA kullanmaktadır. Metropolis versiyonu ile birlikte kullanıcılar ECDSA kullanmak zorunluluğundan kurtulmuş olup kuantum bilişime dirençli Lamport ya da herhangi başka bir teknoloji kullanabilmektedir. • Yüksek (3)
Kullanım amacına ilişkin özellikler	
Uygulama türü	• Genel amaçlı (1)
Akıllı sözleşme desteği	Akıllı sözleşme kavramını ilk ortaya atan ve başarılı biçimde uygulayan platformdur.

	• Evet (1)
Akıllı sözleşme dil desteği	Solidity, Vyper, Yul, Yul+ Solidity: C++ ve JavaScript'ten esinlenerek yaratılmış bir dildir. Diğer sözleşmelere aktarılabilecek kalıtım (inheritance), farklı sözleşmelerden çağırılabilecek yeniden kullanılabilir kodlar (library) ve karmaşık kullanıcı tanımlı türler tanımlanması özelliklerine sahiptir. Başlangıç düzeyindeki kullanıcılara uygun olup kullanımı en yaygın olan akıllı sözleşme geliştirme dilidir. Vyper: Phytonik programlama dilidir. Güçlü yazım, küçük ve anlaşılır derleyici kodu ile sözleşmeleri daha güvenli ve daha kolay denetlenebilir kılmak amacıyla kasıtlı olarak Solidity'den daha az özelliğe sahip olarak geliştirilmiştir. Diğer sözleşmelere aktarılabilecek kalıtım (inheritance), farklı sözleşmelerden çağırılabilecek yeniden kullanılabilir kodlar (library) ve karmaşık kullanıcı tanımlı türler tanımlanması gibi özelliklere sahip değildir. Akıllı sözleşme yazmak isteyen Python geliştiricileri için uygundur. Daha hızlı prototip yaratmayı sağlayan daha az sayıda özelliğe sahiptir. Yul: Ethereum konusunda yeni olup henüz akıllı sözleşmeler konusunda kodlama yapmamış olanlar için Solidity ve Viper önerilmektedir. Basit ve işlevsel düşük seviyeli bir dildir. Sözleşmelerin gas kullanımını optimize etmeye yardımcı olabilecek biçimde ham Ethereum Sanal Makinesine daha yakın bir düzeyde olmayı sağlar. Akıllı sözleşmeler için güvenliği en iyi olan uygulamalara ve EVM ile çalışma detaylarına aşina olunması durumunda Yul ve Yul+ önerilmektedir. Yul orta düzeyli, Yul+ ise düşük düzeyli bir dildir.
Token kullanımı	Ethereum platformu token kullanımını desteklemektedir. • Evet (1)
Niteliksel özellikler	
Olgunluk	İlk olarak 2013 yılında duyurulmuş, 2014 yılında İlk Dijital Para Arzı gerçekleştirilerek 2015'te ilk versiyonu kullanıma sunulmuştur. Kriptopara pazarında ikinci sırada yer alması, birçok farklı projede altyapısından ve akıllı sözleşme özelliğinden faydalanılması nedenleriyle olgunluk düzeyi "çok yüksek" (5) olarak değerlendirilmektedir.
Pazardaki popülarite	Bitcoin'in ardından piyasa değeri bakımından yaklaşık %11'lik payı ile ikinci sırada olup popülaritesi "çok yüksek" (5) olarak değerlendirilmektedir.
Geliştirici	Ethereum Vakfı tarafından desteklenen, açık kaynak kodlu ve herkese açık bir blokzincir platformudur.
Güvenilirlik	Olgunluk, popülarite ve geliştirici özellikleri dikkate alınarak "çok yüksek" (5) olarak değerlendirilmektedir.

- Hyperledger

Farklı alanlarda blokzincir teknolojisinin kullanılabilmesi için ortak çabayla geliştirilmiş olan küresel ve açık kaynak kodlu bir platformdur. İlk olarak 2015 yılı Aralık ayında 17 kuruluş tarafından duyurulmuştur. Linux Vakfının öncülüğünde, sağlık, üretim, finans, lojistik ve teknoloji sektöründeki endüstri liderleri tarafından desteklenmektedir. Hyperledger şemsiyesi altında dağıtık kayıt defteri çerçeveleri, akıllı sözleşme motorları, istemci kütüphaneleri, grafik arayüzleri, yardımcı program kütüphaneleri ve örnek uygulamalar gibi birçok proje desteklenmektedir. Hyperledger çatısı altında yer alan bu projeler; izin gerektiren bir Ethereum akıllı sözleşme blokzinciri olan Burrow, Golang dilinde bir dağıtık kayıt defteri olan Fabric, merkezsizleşmiş kimlikler için oluşturulmuş bir

dağıtık kayıt defteri olan Indy, C++ dilinde bir dağıtık kayıt defteri olan Iroha ve Python dilinde hazırlanmış bir dağıtık kayıt defteri olan Sawtooth'tur.

Tüm Hyperledger projeleri modüler, genişletilebilir, güvenli, tokendan bağımsız ve birlikte çalışabilir işletme dostu çözümler geliştirmeyi hedeflemektedir. Bunun yanı sıra zengin bir Uygulama Programlama Arayüzü (API) kümesi sağlayarak uygulamaların ve kullanıcıların blokzincir ile etkileşime girmelerine yardımcı olmaktadır. Bu amaçlar doğrultusunda Hyperledger mimarisini oluşturan katmanlar aşağıdaki biçimdedir (Dinh, ve diğerleri, 2018):

- Dağıtık kayıt defteri katmanı: Blokzincirin ve her eş tarafından yürütülen verilerin durumunun depolandığı bileşenleri içerir. Aşağıdaki alt bileşenlere sahiptir:
  - İletişim: Düğümler arasındaki eşten eşe mesajlaşmadan sorumludur.
  - Mutabakat: Bloğu oluşturan işlemler kümesinin sırası ve doğruluğu üzerinde anlaşma sağlanan bileşendir.
  - Kripto soyutlama: Diğer modüllerin işleyişini etkilemeden farklı kriptografik algoritmaların veya modüllerin değiştirilmesine izin verir.
  - Kayıt defteri depolama: Veri depolamayı ve farklı modüller arasında farklı veri depolarını sağlar.
- Akıllı sözleşme katmanı: İşlem taleplerinin işlenmesinden ve iş mantığını çalıştırarak işlemlerin geçerli olup olmadığını belirlemekten sorumludur.
- Üyelik katmanı: İzin gerektiren bir ağdaki kimliklerin doğrulanması, yetkilendirilmesi ve yönetilmesinden sorumludur.

Belirlenmiş olan değerlendirme kriterlerine göre Hyperledger platformunun dört temel projesinin özellikleri Çizelge 2.10'da verilmiştir.

Çizelge 2.10. Hyperledger platformunun başlıca projelerinin (Fabric, Sawtooth, Iroha, Indy) özellikleri

Hyperledger	
Teknik özellikler	
Ağa katılım	İzin gerektiren (1)
Blokzincir tipi (açık, özel)	Özel (2)
Hash fonksiyonu	SHA-256 (Fabric, Indy), SHA-512 (Sawtooth, Iroha)
Mutabakat mekanizması	Hyperledger Fabric, Indy, Iroha ve Sawtooth'ta farklı mutabakat protokolleri kullanmaktadır: **Hyperledger Fabric:** İzin gerektiren, oylamaya dayalı bir algoritma olan Apache Kafka kullanılmaktadır. Bileşenlerin arızalanması durumunda sistemin hala doğru

	bir şekilde fikir birliğine ulaşabildiği bir esneklik düzeyi olan kilitlenme hatası toleransına (Crash Fault Tolerance) sahiptir. Ancak Bizanslı hata toleransına karşı toleransı yoktur. **Hyperledger Indy:** Redundant Bizanslı Hata Toleransı (RBFT) adı verilen mutabakat mekanizması kullanılmaktadır. Bizanslı hata toleransına sahiptir. İşlem kesinliği (finality) birkaç saniye içinde gerçekleşir. Ancak, ağda ne kadar çok düğüm varsa mutabakata varmak o kadar uzun sürer. Ağdaki tüm düğümlerin biliniyor ve birbirlerine tamamen bağlı olmaları gereklidir. **Hyperledger Iroha:** Sumeragi adı verilen, izin gerektiren bir sunucu itibar sistemi olan mutabakat algoritması kullanılmaktadır. Bizanslı hata toleransına sahiptir. İşlem kesinliği (finality) birkaç saniye içinde gerçekleşir. Petabaytlarca veri birçok küme arasında dağıtılmıştır. Ancak; ağdaki düğüm sayısı arttıkça mutabakat süresi uzamaktadır. Ağdaki tüm düğümlerin biliniyor ve birbirlerine tamamen bağlı olmaları gereklidir. **Hyperledger Sawtooth**: Geçen Zamanın İspatı (PoET) mutabakat algoritması kullanılmaktadır. Bu mutabakat algoritması ölçeklenebilirlik ve Bizanslı hata toleransı sağlamaktadır. Çözülmesi gereken çatallanma sorunları nedeniyle işlem kesinliği zaman alabilir.
Yazılım dili	Hyperledger projesi Github'da Fabric, Iroha, Sawtooth projelerini de içeren 163 depoya sahiptir. En fazla kullanılan yazılım dilleri Python, Go, Rust, JavaScript, Java olup bunlar dışında içerdiği projelerde C#, C++, HTML gibi birçok dil kullanılmaktadır. **Fabric**: En yaygın kullanılan yazılım dilleri Python, Go, Rust, JavaScript ve Java'dır. **Indy**: En yaygın kullanılan yazılım dilleri Python, Go, Rust, Html, TypeScript ve Apache 2.0'dır. **Iroha**: En yaygın kullanılan yazılım dilleri C++, Python, JavaScript, Java, Shell ve Apache 2.0'dır. **Sawtooth**: En yaygın kullanılan yazılım dilleri Rust, Go, Swift, JavaScript, Java, C#, C++, Python, TypeScript ve Apache 2.0'dır.
Yazılım tipi	Hyperledger projesi açık kaynaklı, modüler ve yapılandırılabilir bir mimariye sahip kurumsal düzeyde bir platformdur.
Performans özellikleri	
İşlem hacmi	Hyperledger Fabric'te 3 500'ten fazla işlem bir saniyeden daha kısa gecikmeyle gerçekleştirilmektedir. Fabric'in yeni versiyonu ile bu sayı yedi katına kadar çıkabilmektedir. Hyperledger özel ve izin gerektiren bir platform olduğundan işlem hacmi açık blokzincir platformlarına göre yüksek olarak değerlendirilmektedir.
Ağ gecikmesi	**Fabric**: İşlemler birkaç saniye içinde kesinleşmektedir. **Indy**: İşlemler birkaç saniye içinde kesinleşmektedir. **Iroha**: İşlemler birkaç saniye içinde kesinleşmektedir. **Sawtooth**: İşlemler birkaç saniye içinde kesinleşmektedir.
Ölçeklenebilirlik (side-chain, sharding, plasma-chain, off-chain)	Hyperledger bünyesindeki blokzincir projeleri özel ve izin gerektiren, kurumsal uygulamalara yönelik çözümler üzerine odaklandığından ölçeklenebilirlik "yüksek" (3) olarak değerlendirilmektedir.
İşlem hızı	İşlemler birkaç saniye içinde tamamlanmakta olup Hyperledger platformu için bu parametre "yüksek" ya da "çok hızlı" olarak değerlendirilmektedir.
Blokzincir üçlü çelişkisi	Hyperledger platformu güvenlik ve ölçeklenebilirlik bakımından güçlü, merkezsizlik bakımından zayıftır. Kurumsal, özel ve izin gerektiren yapısı nedeniyle açık blokzincir platformlarına göre merkezsizlik özelliği düşüktür. • Ölçeklenebilir ve güvenli ama merkezi (1)
Güvenliğe ilişkin özellikler	
DoS ve DDoS saldırılarına direnç	Klasik açık ve izin gerektirmeyen platformlar işlemlerin gerektirdiği maliyet ve dağıtık yapıları nedeniyle DDoS saldırılarına karşı dirençlidir. Hyperledger platformu özel ve izin gerektiren bir ağ olmakla birlikte DDoS saldırılarına karşı dirençlidir (3).
Sybil saldırısına direnç	İzin gerektiren bir ağ olduğundan Sybil saldırısına karşı direnci "yüksek" (3) olarak değerlendirilmektedir.

Kuantum bilişim riskine direnç	Hyperledger Fabric ve Sawtooth'ta kullanılan ECDSA kuantum bilişim riskine karşı dirençli değildir (1). NIST tarafından önerilen kuantum sonrası kriptografi için dijital imza altyapısı qTESLA'nın yakın dönemde hibrit bir çözüm olarak kullanılabileceği tahmin edilmektedir.
Mahremiyet ve gizlilik teknolojisi	Hyperledger asimetrik kriptografi (PKI), sıfır bilgi kanıtı, işlem verilerinin zincir üzerindeki kayıtlardan ayrılması, dijital sertifika yönetimi, çok kanallı tasarımla bilgilerin farklı kanallar arasında ayrılması, aynı kanal içindeki farklı kuruluşlar arasında özel verilerin izolasyonu gibi yöntemlerle gizlilik ve mahremiyeti sağlamaktadır. Hyperledger projelerinin mahremiyet ve gizlilik özelliği "yüksek" (3) olarak değerlendirilmektedir.
Kullanım amacına ilişkin özellikler	
Uygulama türü	**Hyperledger Fabric**: Finansal hizmetler, IoT, sağlık hizmetleri, ilaç satış ve takibi, tedarik zinciri, kamu hizmetleri başta olmak üzere özel ve izin gerektiren merkezi olmayan kurumsal uygulamalarda kullanılabilmektedir. • Genel amaçlı (1) **Hyperledger Indy**: Kendi kendini yöneten kimlik yönetimi için özel olarak geliştirilmiştir. Kullanım alanları arasında dijital belgeler, şifresiz kimlik doğrulama, spam engelleme, üyelik yönetimi, yaş kısıtlamaları, zafiyet uyarısı, işe alımda aday doğrulama, tedarik zincirinde menşei sorgulama yer almaktadır. **Hyperledger Iroha**: Güçlü olduğu konu KYC gibi hesaplar roller ve erişim haklarının yönetimini gerektiren kullanım senaryolarıdır. Iroha'nın kullanılabileceği başlıca alanlar arasında dijital varlıkların, kimliklerin ve veri serilerinin yönetilmesi, bankalar arası ödemeler, merkez bankası destekli dijital para birimleri, ödeme sistemleri, ulusal kimlikler ve lojistik yer almaktadır. **Hyperledger Sawtooth**: Dağıtık kayıt defterlerinin ölçeklenebilirlik, güvenlik ve mahremiyet kaygılarını gidermek üzere tasarlanmıştır.
Akıllı sözleşme desteği	Ethereum'daki akıllı sözleşmeler, Hyperledger'da Chaincode olarak adlandırılmaktadır. Akıllı sözleşme desteği sağlamaktadır. • Evet (1)
Akıllı sözleşme dil desteği	JavaScript, Java, Go ve Node.js gibi genel amaçlı programlama dilleri ile akıllı sözleşme geliştirmeyi desteklemektedir.
Token kullanımı	Tokenden bağımsız bir platformdur. • Hayır (2)
Niteliksel özellikler	
Olgunluk	Olgunluk düzeyi "çok yüksek" (5) olarak değerlendirilmektedir.
Pazardaki popülarite	Hyperledger.org adresinde yayınlanmış olan (https://www.hyperledger.org/wp-content/uploads/2018/08/HL_Whitepaper_IntroductiontoHyperledger.pdf) tanıtım dokümanına göre, 2018 yılı Ağustos ayı itibarıyla içlerinde Airbus ve VMware gibi firmaların da olduğu 230 üye, 3,6 milyon satır koda sahip 10 projeye sahiptir. Tüm bu özellikleri, arkasındaki güçlü kurumsal destek ve kurumsal uygulamalardaki yaygın kullanımı nedenleriyle popülaritesi "çok yüksek" (5) olarak değerlendirilmektedir.
Geliştirici	İlk olarak 2015 yılı Aralık ayında 17 kuruluş tarafından duyurulmuştur. Linux Vakfının öncülüğünde, sağlık, üretim, finans, lojistik ve teknoloji sektöründeki endüstri liderleri tarafından desteklenmektedir.
Güvenilirlik	Olgunluk, popülarite ve geliştirici özellikleri dikkate alınarak "çok yüksek" (5) olarak değerlendirilmektedir.

Hyperledger Fabric

Hyperledger Fabric kurumsal uygulamalar geliştirmek için uygun olan bir açık kaynak kodlu blokzincir platformudur. Yetkilendirilmiş kimlikler ve tüm katılımcıların bilindiği izin gerektiren ağlarda dağıtık kayıt defteri çözümlerini desteklemektedir.

Modüler bir mimariye sahip olan Hyperledger Fabric blokzincir uygulamalarının esnekliğini ve direncini maksimize etme potansiyeline sahiptir. Bu platformda üyeler birbirlerini tanımakta ancak aralarındaki işlemler gizli kalmaktadır. Eklenip çıkarılabilir mimari bileşenleri şifreleme ve mutabakatı içermektedir. Tasarımcıya kimlik, mutabakat ve şifreleme için spesifik algoritmalar kullanma özgürlüğü veren modüler yapısı nedeniyle yüksek derecede esneklik ve ölçeklenebilirlik sunmaktadır.

Hyperledger Fabric akıllı sözleşmeleri desteklemekte ve bu özellik "Chaincode" olarak adlandırılmaktadır. Bir Chaincode herhangi bir programlama dilinde yazılabilmekte ve ayrıca işletilebilmektedir. Chaincode'u tamamen destekleyen ilk dil Golang'tır.

Eğer tüm herkesin erişimine açık olmayan, merkezi olmayan bir kurumsal çözüm geliştirilecekse proje için Hyperledger Fabric seçilmelidir.

Hyperledger Sawtooh

Hyperledger Fabric'e benzer olarak, Hyperledger Sawtooth da izin gerektiren blokzincir ağlarında uygulama geliştirmek için tasarlanmıştır. Intel tarafından geliştirilmiş olup Geçen Zamanın İspatı (Proof of Elapsed Time - PoET) adı verilen bir mutabakat algoritmasını kullanmaktadır. Bu mutabakat algoritması aşağıdaki stratejiyi izlemektedir:

- Blokzincir ağındaki her katılımcı rastgele bir zaman süresince beklemektedir.
- Bekleme zamanını ilk tamamlayan katılımcı yeni bloğun lideri olmaktadır.

Bu mutabakat mekanizması iki koşulun uygun biçimde karşılanmasını gerektirmektedir. Birincisi; kazanan bekleme zamanını rastgele olarak seçmiş midir veya bir üye liderliği ele geçirmek için kasıtlı olarak daha kısa bir süre seçebilir mi? İkinci olarak; kazanan gerçekten belirlenmiş olan bekleme zamanını tamamlamış mıdır?

Hyperledger Sawtooth'daki akıllı sözleşmeler Python, Go, Javascript, Rust gibi farklı programlama dillerinde yazılabilir ve ilgili IDE'lerde kullanım için dağıtılabilir. Dağıtık kayıt defterlerinin ölçeklenebilirlik, güvenlik ve mahremiyet kaygılarını gidermek üzere tasarlanmıştır.

Hyperledger Iroha

Dağıtık kayıt defteri teknolojisi gerektiren altyapı projelerine dâhil edilebilen bir iş blokzincir çerçevesidir. Fabric ile benzer ilkeleri izlemekte olup web ve mobil uygulama geliştiricilerinin Hyperledger projesine katkıda bulunabileceği bir geliştirme ortamı sağlamayı amaçlamaktadır. Basit yapılı, modüler, etki alanına dayalı bir C++ tasarımına sahiptir ve YAC adı verilen yeni, çökmeye karşı toleranslı bir fikir birliği algoritmasına sahiptir.

Iroha Japon Kaizen prensibinden esinlenen basit bir dağıtık kayıt defteri teknolojisidir. Varlık, bilgi ve kimlik yönetimi gereksinimleri için temel işlevlere sahip verimli, güvenilir ve çökmeye karşı dayanıklı bir araçtır. Para birimleri ve altın gibi özel varlıkların oluşturulması ve yönetimi, kullanıcı hesaplarının yönetimi, sistemdeki etki alanlarına göre hesapların sınıflandırılması, sistemdeki işlemlerin ve sorguların yürütülmesi için hakların ve kullanıcı izinlerinin doğrulanması sistemi, sistemdeki işlemler ve sorgular için iş kurallarının doğrulanması ve çoklu imza işlemleri gibi özelliklere sahiptir.

Bitcoin ve Ethereumdan temel farkı yerel bir kripto para biriminin olmaması ve izin gerektirmesidir. Ayrıca, önceden oluşturulmuş komutlar kullanılarak dijital varlıkların yaratılması ve transferi gibi ortak fonksiyonların gerçekleştirilmesine izin vererek nispeten basit işler için akıllı sözleşme yazma ihtiyacını ortadan kaldırır.

Diğer Hyperledger platformlarından farkıysa yüksek performanslı ve düşük gecikmeli işlemlere izin veren YAC adlı yeni mutabakat algoritması ve bazı ortak görevler için sahip olduğu önceden tanımlanmış yerleşik komutlardır. Son olarak, tüm komutlar, sorgular ve ağa katılım için izinlerin ayarlanmasına izin veren sağlam bir izin sistemine sahip tek platformdur.

Hyperledger Indy

Hyperledger Indy blokzincirler ve diğer dağıtık kayıt defterleri için dijital kimlikler sağlamak üzere araçlar, kitaplıklar ve yeniden kullanılabilen bileşenler sağlamaktadır. Böylelikle yönetim alanları, uygulamalar ve veri yığınları arasında birlikte çalışabilirliğin sağlanması hedeflenmektedir. Indy diğer blokzincir çözümleri ile birlikte çalışabileceği gibi

bağımsız olarak da kullanılabilmektedir. Kendi kendini yöneten kimlik yönetimi için özel olarak geliştirilmiştir. Sıfır bilgi (zero-knowledge) kriptografi ve gelişmiş bir Bizanslı Hata Toleransı (RBFT) mutabakat algoritmasını kullanmaktadır. Kullanım alanları arasında dijital belgeler, şifresiz kimlik doğrulama, spam engelleme, üyelik yönetimi, yaş kısıtlamaları, zafiyet uyarısı, işe alımda aday doğrulama, tedarik zincirinde menşei sorgulama yer almaktadır.

Hyperledger Burrow

Hyperledger Burrow, basitlik, hız ve geliştirici ergonomisine odaklanan bir blokzincir çözümüdür. Hem Ethereum Sanal Makinesi (EVM) hem de WebAssembly (WASM) tabanlı akıllı sözleşmeleri desteklemekte, Tendermint algoritması aracılığıyla BFT mutabakat algoritmasını kullanmaktadır. Gelişmiş bir olay sistemine sahiptir ve zincir üzerindeki verilerin ilişkisel bir veritabanı eşlemesini gerçekleştirebilmektedir. Yönetim ve izin, yerleşiktir ve zincir üzerinde teklif işlemleri ile değiştirilebilir. Açık ve izin gerektiren Hisse İspatı kullanımı ve özel/konsorsiyum ağları için uygundur.

Burrow'un temel amacı sadece ihtiyaç duyulan özellikleri sağlayarak merkezi olmayan, açık, izin gerektiren basit bir blokzincir çözümü sağlamaktır. Akıllı sözleşmeleri desteklemektedir. Geliştiricilerin herhangi bir orkestrasyon desteği kullanmadan dizüstü bilgisayarlarında ya da sunucularında geliştirme yapmalarına olanak verir (Davis S. , 2019).

- Stellar

Ethereum'un çok kapsamlı yetenekleri olsa da, bazı uygulamalar için bu özelliklerin sadece bir kısmı gereklidir. Karmaşık akıllı sözleşme desteği ve Turing tamlığı bazen gereksiz hale gelebilmektedir. Çoğu İlk Kripto Para Arzı için Ethereum'un tüm özellikleri değil sadece temel tokenler yeterlidir. Ödemeler gibi belirli alanlarda yüksek performans ve kullanılabilirlik için geliştirilmiş ve özelleştirilmiş birçok platform mevcuttur. Stellar bankaları, ödeme sistemlerini ve insanları birbirlerine bağlayarak hızlı, güvenilir ve uygun maliyetli para transferi sağlayan, bu tip özelleştirilmiş bir platformdur.

Stellar'da da hesaplar Ethereum'da olduğu gibi merkezi veri tabanı yapısındadır. Stellar kayıt defteri ağdaki her bir hesaba ait tüm bakiye ve işlemlerin bir listesini tutar. Ayrıca,

dâhili olarak her bir para birimi-ihraççı çifti için teklifleri içeren bir sipariş defteri de tutulur. Bu sayede kullanıcı spesifik bir sipariş defterinde banka adı-para biriminden firma adı-Bitcoin'e kur durumunu görebilir. Böylelikle kullanıcılar hem geleneksel döviz işlemlerine benzer biçimde para alıp satabilir, hem de işlemler esnasında para birimi dönüşümü sorunsuz biçimde gerçekleşir.

Kayıt defterinin bir kopyası Stellar Mutabakat Protokolünü uygulayan, dünyanın dört bir yanına dağılmış kuruluşlar ve bireyler tarafından kullanılan, Stellar Core çalıştıran her bir sunucuda tutulur. Stellar ağında kullanıcılar ödeme işlemlerine yönelik kendi uygulamalarını geliştirebilmekte, bu uygulamalar Stellar ağı içerisinde Horizon adı verilen sunucu vasıtasıyla etkileşim kurabilmektedir. Kullanıcılar Horizon ile iletişimi web tarayıcı, komut ekranı ya da Stellar SDK adlı Java, JavaScript ve Go programlama dillerini destekleyen arayüz ile sağlayabilmektedir.

Stellar platformu açık kaynak kodlu, dağıtık ve topluluğa ait bir teknolojidir. Stellar ağında kullanıcıdan depozit alarak kullanıcının hesabına karşılığında para yatıran, kullanıcıların kendilerine verilen bu krediyi alarak para çekmelerine izin veren güvenilir kuruluşlar Anchor olarak adlandırılmaktadır. Stellar ağında tüm para transferleri bu biçimde gerçekleştirilmektedir.

Stellar daha küçük transferlerin maliyetini düşürmek ve artımlı ödeme seçenekleri sunmak, havale maliyetlerini düşürmek ve mobil para platformlarını birlikte çalışabilir hale getirmek için kullanılmaktadır. Stellar platformunun özellikleri Çizelge 2.11'de verilmiştir.

Çizelge 2.11. Stellar platformunun özellikleri

Stellar	
Teknik özellikler	
Ağa katılım	Ağda farklı düğüm rolleri mevcuttur ve doğrulama yetkisi için güvenilirlik ve itibara dayalı bir mekanizma bulunmaktadır (izin veren bir mekanizma yoktur). İşlemlerin hızlı olması için düğümlerin küçük bir bölümü doğrulama görevini yürütür. • İzin gerektirmeyen (2)
Blokzincir tipi (açık, özel)	Açık (1)
Hash fonksiyonu	SHA-256
Mutabakat mekanizması	Stellar Mutabakat Protokolü (SCP) – Federe Bizanslı Anlaşması algoritmasından türetilmiştir
Yazılım dili	https://github.com/stellar/stellar-core adresinde yer alan verilere göre (Ekim 2022 itibariyle), 86 geliştirici tarafından katkı verilen kaynak kodda kullanılan yazılım

	dilleri ve her birinin oranı şu biçimdedir: C (%53,1), C++ (%45,4), RPC (%0,5), M4 (%0,4), Shell (%0,2), Rust (%0,2)
Yazılım tipi	Açık kaynak kodlu (1)
Performans özellikleri	
İşlem hacmi	1 000'den fazla işlem/sn
Ağ gecikmesi	3 – 5 saniye, Çok düşük
Ölçeklenebilirlik (side-chain, sharding, plasma-chain, off-chain)	Herhangi bir kod değişikliği gerekmeden, parametre değişikliği ile saniyedeki işlem sayısı 4 000'e çekilebilmektedir. • Yüksek (3)
İşlem hızı	3 – 5 saniye
Blokzincir üçlü çelişkisi	Ölçeklenebilir ve güvenli, ancak 70'in biraz üzerinde doğrulayıcı düğüm ile daha az merkezidir. • Ölçeklenebilir ve güvenli ama merkezi (1)
Güvenliğe ilişkin özellikler	
DoS ve DDoS saldırılarına direnç	• Yüksek (3)
Sybil saldırısına direnç	• Yüksek (3)
Kuantum bilişim riskine direnç	• Düşük (1)
Mahremiyet ve gizlilik teknolojisi	Bitcoin sistemine benzer biçimde redshift adlı araçla yeni adresler tanımlanarak bir derece mahremiyet sağlanmaktadır. Ancak, önceki adresler izlenerek yapılan işlemlerin izi sürülebilmektedir. • Yüksek (3)
Kullanım amacına ilişkin özellikler	
Uygulama türü	İşlem ücreti çok düşük, işlem hızı yüksek sınır ötesi varlık ve para transferi için kullanılmaktadır. Kendi kripto para birimi Lümen (XLM) olarak adlandırılır. • Sadece belirli işlemler için (2)
Akıllı sözleşme desteği	Stellar Akıllı Sözleşmeleri (SSC) adı verilen akıllı sözleşme oluşturulabilir.
Akıllı sözleşme dil desteği	SSC adlı özel akıllı sözleşme yapısında Çoklu imza, Batch/Atomicity, Sıra, Zaman sınırları parametreleri kullanılarak tanımlama yapılmaktadır. • Evet (1)
Token kullanımı	Token görevi de gören kendi para birimine sahiptir (XLM) • Evet (1)
Niteliksel özellikler	
Olgunluk	2014 yılında kurulmuş, açık kaynak kodlu, pazar payı bakımından onuncu sırada yer alan bir platform olarak olgunluk düzeyi "çok yüksek" (5) olarak değerlendirilmektedir.
Pazardaki popülarite	• Yüksek (4)
Geliştirici	Jed McCaleb ve Joyce Kim tarafından başlatılmış olmakla birlikte Stellar Development Foundation tarafından işletilmektedir.
Güvenilirlik	Olgunluk, popülarite ve geliştirici özellikleri dikkate alınarak "yüksek" (4) olarak değerlendirilmektedir.

- Quorum

Kurumsal bir Ethereum sürümü olan Quorum blokzincir teknolojisinin özellikle finans sektöründe kullanımı konusuna odaklanmaktadır. JP Morgan tarafından geliştirilen bir çözüm olan Quorum finans sektörü için en önemli özellikler olan hızlı çalışma, yüksek verimlilik ve kullanıcı mahremiyetinin korunması konularında öne çıkmaktadır.

Belirlenmiş olan değerlendirme kriterlerine göre Quorum platformunun özellikleri Çizelge 2.12'de verilmiştir.

Çizelge 2.12. Quorum platformunun özellikleri

Quorum	
Teknik özellikler	
Ağa katılım	İzin gerektiren (1)
Blokzincir tipi (açık, özel)	Özel (2)
Hash fonksiyonu	SHA3-512 ve Keccak-256 kullanılabilmektedir.
Mutabakat mekanizması	Oy tabanlı QuorumChain Raft ve İstanbul BFT kullanılmaktadır. İstanbul BFT bir Bizanslı Hata Toleransı mutabakat algoritmasıdır. Düğümlerin %30'a kadarı kötü niyetli olsa da zinciri koruyabilmektedir.
Yazılım dili	https://github.com/ConsenSys/quorum adresinde yer alan verilere göre (Ekim 2022) aktif 490 geliştirici tarafından katkı verilen kaynak kodda kullanılan yazılım dilleri ve her birinin oranı şu biçimdedir: Go (%89,1), C (%4,6), JavaScript (%3,0), Solidity (%1,6), Assembly (%0,6), Java (%0,2) ve diğer (%0,9)
Yazılım tipi	Açık kaynak kodludur. Kullanılan lisans, Ethereum'a benzer GPL/LGPL'dir. Herhangi bir sınırlama olmadan indirilebilir, değiştirilebilir ve dağıtılabilir.
Performans özellikleri	
İşlem hacmi	Performans konusunda güçlüdür. Saniyede yüzlerce işlem gerçekleştirilebilir. Bu rakam optimizasyon ile önemli ölçüde iyileştirilebilmektedir.
Ağ gecikmesi	50 ms'lik blok üretim hızı ile çok hızlı işlem yapılmasını sağlar.
Ölçeklenebilirlik (side-chain, sharding, plasma-chain, off-chain)	Özel ve izin gerektiren bir platform olması ve kullandığı mutabakat algoritmasının özelliğine dayalı olarak ölçeklenebilirliği "yüksek"tir (3). Ağ performansını ve verimliliği artırmak için sharding teknikleri kullanılır.
İşlem hızı	Çok yüksektir
Blokzincir üçlü çelişkisi	Ölçeklenebilir ve güvenli, ancak daha az merkezidir. • Ölçeklenebilir ve güvenli ama merkezi (1)
Güvenliğe ilişkin özellikler	
DoS ve DDoS saldırılarına direnç	TLS karşılıklı kimlik doğrulaması devre dışı bırakılırsa savunmasızdır. • Düşük (1)
Sybil saldırısına direnç	Saldırıların gerçekleştirilmesi bir maliyet getirdiğinden Sybil saldırılarına karşı direnci "yüksek" (3) olarak nitelendirilmektedir.
Kuantum bilişim riskine direnç	• Düşük (1)
Mahremiyet ve gizlilik teknolojisi	Mahremiyet ve güvenliği sağlamak için Sıfır Bilgi Güvenlik Katmanı kullanılır. Özel akıllı sözleşmelerin durumu ve çalışması sadece taraflara veya onaylanmış üçüncü taraflarca bilinir. Çeşitli bulut sağlayıcılarında güvence altına alınabilen veya yerel diskte şifrelenebilen özel bir anahtar kullanarak işlemleri imzalayarak özel anahtar yönetimini işlem doğrulamasından ayıran işlem imzalayıcısı olan EthSigner kullanılır. Tüm veri gizliliği, kriptografi ve segmentasyon yoluyla elde edilir. Kriptografi, işlemlerle ilgili verilere (herkesin blokzincirde gördüğü) uygulanır. Segmentasyon, her düğümün yerel durum veritabanına uygulanır (depolama sözleşmesini içerir ve yalnızca düğüm tarafından erişilebilir). Yalnızca özel taraf işlemlerine yönelik düğümler, özel sözleşme işlemleriyle ilişkili kodu yürütebilir, bu da yerel durum veri tabanındaki özel sözleşme veri depolamasının güncellenmesiyle sonuçlanır. Sonuç olarak, her düğümün yerel durum veritabanı yalnızca taraf oldukları genel ve özel verilerle doldurulur. • Yüksek (3)
Kullanım amacına ilişkin özellikler	
Uygulama türü	En güçlü olduğu ve ortaya çıkarılma amacı finans sektörüdür. • Sadece belirli işlemler için (2)

Akıllı sözleşme desteği	Ethereum'a dayalı olduğundan akıllı sözleşmeleri desteklemektedir (1). Bir akıllı sözleşme özel (private) olarak ayarlandıktan sonra açık hale dönüştürülemez. Aynı biçimde, açık olarak yaratılmış akıllı sözleşmeler de daha sonra özel hale getirilemezler.
Akıllı sözleşme dil desteği	Solidity
Token kullanımı	Ethereum tabanlı olduğundan ERC-20 token hizmeti kullanılabilmektedir (1).
Niteliksel özellikler	
Olgunluk	Ethereum'a dayandığından ve Ethereum blokzincirin tüm özelliklerine sahip olduğundan olgunluk düzeyi "yüksek" (4) olarak değerlendirilmektedir.
Pazardaki popülarite	Yüksek (4)
Geliştirici	JP Morgan ve Ethereum geliştiricileri
Güvenilirlik	Olgunluk, popülarite ve geliştirici özellikleri dikkate alınarak "yüksek" (4) olarak değerlendirilmektedir.

- Corda

Bankalar tarafından oluşturulmuş R3 adlı bir konsorsiyum tarafından yönetilen Corda bankalar ve finans kuruluşlarına en uygun blokzincir platformudur. Daha çok bankalar için gizlilik ve güvenlik konularına odaklanmış olmakla birlikte birçok farklı kullanım alanı da bulunmaktadır.

Corda ile diğer blokzincir çözümleri arasındaki farklardan biri noter adı verilen düğümlerin kullanılmasıdır. Noter adı verilen bu düğümler madencilere benzer şekilde hareket ederler ve işlemleri doğrulama sorumluluğunu taşırlar.

Belirlenmiş olan değerlendirme kriterlerine göre Quorum platformunun özellikleri Çizelge 2.13'te verilmiştir.

Çizelge 2.13. Corda platformunun özellikleri

Corda (Hearn ve Brown, 2019)	
Teknik özellikler	
Ağa katılım	İzin gerektiren (1)
Blokzincir tipi (açık, özel)	Özel (2)
Hash fonksiyonu	İmza algoritması olarak SHA256withRSA, SHA256withECDSA ve BPQS (Blockchained Post-Quantum Signatures) kullanılmaktadır.
Mutabakat mekanizması	Corda ağında işlemler noter adı verilen, ağa eklenip çıkarılabilen düğümlerce ayrıştırılır. Yani, herhangi bir mutabakat algoritmasına bağımlı değildir.
Yazılım dili	https://github.com/corda/corda adresinde açık kaynak kodlu olarak sunulan yazılımın Ekim 2022 itibariyle 192 geliştiricisi bulunmaktadır. Yazılım büyük oranda (%94,3) Kotlin ile geliştirilmiş olup diğer diller ve oranları Java (%2,6), C++ (%2,1), Python (%0,3), Groovy (%0,2), Shell (%0,3) ve diğer (%0,2) biçimindedir.

	Düğümler ilişkisel bir veritabanı ile desteklenmekte ve deftere yerleştirilen veriler SQL kullanılarak sorgulanabilmekte, özel tablolarla birleştirilebilmektedir.
Yazılım tipi	Açık kaynak kodlu olarak Github'da sunulmaktadır.
Performans özellikleri	
İşlem hacmi	Tek bir düğümün gerçekleştirdiği işlem saniyede 800 olup çok noterli bir ağda bu sayı saniyede 20 000'e çıkabilmektedir. İşlem hacmi "çok yüksek" olarak değerlendirilmektedir.
Ağ gecikmesi	Bir mutabakat protokolü kullanılmadığından ağ gecikmesi "çok düşük"tür.
Ölçeklenebilirlik (side-chain, sharding, plasma-chain, off-chain)	Paralel olarak çalışan yeni noterler çevrimiçi hale getirilerek sistemin ölçeklenebilirliği artırılabilmektedir. Diğer sistemlere göre daha iyi bir ölçeklenebilirlik sağlanmaktadır. Klasik sistemlere kıyasla daha iyi bir ölçekleme için kısmi görünürlük (düğümlerin sadece kendilerinin dâhil olduğu işlemlerle karşılaşmaları), çok sayıda noter, paralel işlem, chain snipping, geçerlilik imzaları, Tam zamanında (JIT) derleme kullanılmaktadır. • Yüksek (3)
İşlem hızı	İşlem hızı noterlerin işlemleri ne sürede gerçekleştirdiğine ve çatışmaları ne kadar sürede çözebildiğine bağlıdır. Diğer platformlara kıyasla tek bir mutabakat mekanizmasına bağımlı olmadığından sisteme eklenen noterlerle işlem hızı artırılabilmektedir. Bu nedenle, işlem hızı "çok hızlı" olarak değerlendirilmektedir.
Blokzincir üçlü çelişkisi	Diğer özel ve izin gerektiren pltformlarda olduğu gibi merkezsizlikten bir miktar feragat edilmektedir. • Ölçeklenebilir ve güvenli ama merkezi (1)
Güvenliğe ilişkin özellikler	
DoS ve DDoS saldırılarına direnç	Kapalı ve izin gerektiren bir ağda çalışması, ağ haritası verilerinin içerik dağıtım ağlarının önbelleğe alınması yoluyla dağıtılabilmesi ve sadece değiştirilen girişlerin düğümler tarafından alınabilmesi gibi nedenlerle DDoS saldırılarına karşı direnci "yüksek"tir (3).
Sybil saldırısına direnç	Corda ağı, üst düzey üyelerin şirket olmasını zorunlu kılmak için kimlik doğrulaması gerçekleştirir ve tüm ağların bunu yapması önerilir. Sybil saldırısına karşı direnci "yüksek"tir (3).
Kuantum bilişim riskine direnç	Dijital imza için R3 bünyesinde geliştirilmiş olan BPQS (Blockchained Post-Quantum Signatures) kuantum bilişim riskine karşı direnci "yüksek"tir (3).
Mahremiyet ve gizlilik teknolojisi	Veriler, bilmesi gereken (need-to-know) bir temelde paylaşılır. Düğümler, talep üzerine başka bir düğüme gönderdikleri bir işlemin bağımlılık grafiğini sağlar, ancak tüm işlemlerin küresel yayını yoktur. • Yüksek (3)
Kullanım amacına ilişkin özellikler	
Uygulama türü	Corda daha çok bankalar için gizlilik ve güvenlik konularına odaklanmıştır. Sağladığı mahremiyet, ölçeklenebilirlik ve hızlı işlem gerçekleştirme özellikleriyle başta finans olmak üzere sağlık hizmetleri, dijital varlıklar, dijital kimlikler, enerji, sigorta ve kamu hizmetlerinde kullanım alanı bulunmaktadır. • Genel amaçlı (1)
Akıllı sözleşme desteği	Corda, CorDapps adı verilen, küresel veritabanını yeni yeteneklerle genişleten uygulamaların yazılması ve yürütülmesi için JVM (Java Virtual Machine) üzerinde çalışan akıllı sözleşmelerin kullanımına imkân vermektedir (1).
Akıllı sözleşme dil desteği	CorDapp Design Language (CDL) adı verilen araçla akıllı sözleşmeler tasarlanmaktadır. Yazılan akıllı sözleşmeler düzyazıya benzer ve bu nedenle kullanım kolaylığı sunar.
Token kullanımı	Platform içerisinde farklı amaçlarla SDK adı verilen tokenların yaratılması ve kullanılması mümkündür (1).
Niteliksel özellikler	
Olgunluk	Corda'nın yaratıcısı R3 2014 yılında kurulmuş, 2015 yılında 42 üyeden oluşan bir konsorsiyum halini almış, Corda'nın ilk sürümü Nisan 2016'da yayınlanmıştır. 2021 yılı Şubat ayında ise Conclave adı verilen, hassas iş verilerini koruyan gizli bir bilgi işlem platformu piyasaya sürülmüştür. Olgunluk düzeyi "yüksek" (4) olarak değerlendirilmektedir.

Pazardaki popülarite	Güçlü R3 konsorsiyumu ve hizmet sunduğu birçok önemli kuruluş nedeniyle popülaritesi “yüksek” (4) olarak değerlendirilmektedir.
Geliştirici	75’ten fazla üyesi olan R3 konsorsiyumu tarafından yönetilmektedir.
Güvenilirlik	Olgunluk, popülarite ve geliştirici özellikleri dikkate alınarak “yüksek” (4) olarak değerlendirilmektedir.

- Multichain

MultiChain, kuruluşlar içinde veya arasında özel blokzincirlerin oluşturulması ve dağıtılması için kullanıma hazır bir platformdur. Bitcoin Core yazılımından türetilmiştir. MultiChain, kullanıcı izinlerinin entegre yönetimi yoluyla madencilik, gizlilik ve açıklıkla ilgili sorunları çözmektedir. Temel amaçlar blokzincir faaliyetinin yalnızca seçilen katılımcılar tarafından görülebilmesini sağlamak, hangi işlemlere izin verileceğine dair kontroller sunmak, madenciliğin iş ispatı ve ilgili maliyetleri olmadan gerçekleştirilmesini sağlamaktır. Özel ve izne tabi olduğundan zincirin katılımcıları maksimum blok boyutunu kontrol edebilmekte ve ölçeklenebilirlik sorunu böylelikle çözülebilmektedir (Greenspan, 2015). MultiChain blokzincir tasarımında ağ özelliklerinin çoğu konfigürasyon ayarları ile belirlenmektedir.

Destek içermeyen, kısıtlı kullanım özelliklerine sahip ücretsiz sürümü yanında farklı ödeme ve destek seçeneklerine sahip sürümleri, ayrıca yine ücreti karşılığı Azure üzerinden sunulan blokzincir çözümü bulunmaktadır.

Belirlenmiş olan değerlendirme kriterlerine göre MultiChain özel blokzincir platformunun özellikleri Çizelge 2.14’te verilmiştir.

Çizelge 2.14. MultiChain blokzincir platformunun özellikleri.

MultiChain	
Teknik özellikler	
Ağa katılım	Her iki tipte de konfigüre edilebilir (3) (herkes katılabilir, sadece bazıları gönderme/alma yapabilir)
Blokzincir tipi (açık, özel)	Her iki tipte de konfigüre edilebilir (3)
Hash fonksiyonu	Gönderme ve alma işlemlerinde P2SH adlı hash fonksiyonu kullanılır. Ancak, bu fonksiyonun kullanımında girdiye bir de “salt” eklenerek sözlük saldırılarına karşı önlem alınır.
Mutabakat mekanizması	PBFT’ye benzeyen, ancak blok başına birden fazla doğrulayıcı yerine tek bir doğrulayıcının olduğu, tanımlanmış blok doğrulayıcılar arasında dağıtılmış bir fikir birliği algoritması kullanılmaktadır. MultiChain'de tüm ayrıcalıklar, özel meta veriler içeren ağ işlemleri kullanılarak verilir ve iptal edilir. İlk "genesis" bloğunun madencisi, diğer kullanıcıların

	ayrıcalıklarını yönetmek için yönetici hakları da dâhil olmak üzere tüm ayrıcalıkları otomatik olarak alır.
Yazılım dili	Yazılım dili olarak PHP, Java, Python, Shell ve JavaScript kullanılmaktadır.
Yazılım tipi	Bitcoin ve Bitcoin Core ile geriye doğru uyumlu açık kaynak kodludur. Kodlara https://github.com/MultiChain adresinden erişilebilmektedir.
Performans özellikleri	
İşlem hacmi	Bitcoin mimarini kullanmakla birlikte, MultiChain'de blok boyutu sınırı çok daha yüksek (1 GB'ye kadar) ve blok süresi çok daha düşük (2 saniyeye kadar) ayarlanabilmektedir. Böylece bu hesaplamaya dayanarak, teoride, saniyede 2 milyonun üzerinde işlem gerçekleştirilebilir. Ancak hâlihazırda çoklu zincir veya Bitcoin protokolü kullanılarak orta sınıf donanımda saniyede 1 000'in biraz üzerinde işlem gerçekleştirilebilmektedir (Blok boyutu 8 MB olarak ayarlanmaktadır).
Ağ gecikmesi	İşlem hacminde olduğu gibi, bu parametre de MultiChain tasarlanırken konfigüre edilmektedir. Bitcoin'deki kadar uzun bekleme süresi gerekmemektedir. Mevcut blok boyutu ve izin gerektiren ağdaki mutabakatın hızı dikkate alındığında birkaç saniyede işlemler tamamlanmaktadır.
Ölçeklenebilirlik (side-chain, sharding, plasma-chain, off-chain)	Özel ve izne tabi olduğundan zincirin katılımcıları maksimum blok boyutunu kontrol edebilmekte ve ölçeklenebilirlik sorunu böylelikle çözülebilmektedir. • Yüksek (3)
İşlem hızı	Birkaç saniyede işlemler tamamlanmaktadır. Çok hızlı olarak değerlendirilmektedir.
Blokzincir üçlü çelişkisi	Yapılan tasarıma göre değişkenlik göstermekle birlikte, özel ve izin gerektiren bir tasarımda merkezsizlikten taviz verilmektedir. • Ölçeklenebilir ve güvenli ama merkezi (1)
Güvenliğe ilişkin özellikler	
DoS ve DDoS saldırılarına direnç	Blokzincir herkese açıksa, hizmet reddi saldırılarını önlemek için "support-miner-precheck" parametresi "true" olarak ayarlanmıştır. Yüksek (3)
Sybil saldırısına direnç	anyone-can-mine=false mining-diversity=0 mining-turnover=1 ayarları içerisinde "mining-diversity"nin 1 yapılması Sybil saldırısına karşı direnç sağlamaktadır ancak bu durumda da sadece bir düğümün bile mevcut olmaması halinde blok ilerlemesi durur. Sonuç olarak, Sybil saldırısına karşı dirençli değildir. • Düşük (1)
Kuantum bilişim riskine direnç	Bitcoin ile aynı derecede dirençlidir. • Yüksek (3)
Mahremiyet ve gizlilik teknolojisi	İşlemler ve düğümler için tek adres yerine çok sayıda adres kullanılması, güvenilir bir üçüncü tarafça işlemler içini bir "karıştırma" işlemi uygulanması, homomorfik şifreleme ve sıfır bilgi ispatı gibi mahremiyet çözümleri desteklenmektedir. • Yüksek (3)
Kullanım amacına ilişkin özellikler	
Uygulama türü	Finansal sistemler, kaynak (menşei) takibi, kuruluşlar arası kayıt tutma, çok taraflı bilgi/veri toplama gibi kullanım senaryoları için uygundur. • Genel amaçlı (1)
Akıllı sözleşme desteği	Ethereum benzeri bir akıllı sözleşme desteği bulunmamaktadır. • Hayır (2)
Akıllı sözleşme dil desteği	-
Token kullanımı	Token yaratılmasını ve yerel kripto para çıkarılmasını desteklemektedir. • Evet (1)
Niteliksel özellikler	
Olgunluk	2015 yılında kurulmuş olup açık kaynak kodlu yapısı, ücretli kurumsal çözümleri ve SAP, Accenture gibi çok sayıda platform ortakları nedeniyle olgunluk düzeyi "yüksek" (4) olarak değerlendirilmektedir.

Pazardaki popülarite	SAP, Accenture gibi çok sayıda platform ve ürün ortakları nedeniyle popülaritesi "yüksek" (4) olarak değerlendirilmektedir.
Geliştirici	MultiChain Coin Sciences Ltd. çatısı altında GPLv3 lisanslı açık kaynak kodlu versiyonu, bu versiyona ilave olarak ücretli sürümleri bulunmaktadır.
Güvenilirlik	Olgunluk, popülarite ve geliştirici özellikleri dikkate alınarak "yüksek" (4) olarak değerlendirilmektedir.

- OpenChain

Openchain, açık kaynaklı bir dağıtık kayıt defteri teknolojisidir. Dijital varlıkları sağlam, güvenli ve ölçeklenebilir bir şekilde yayınlamak ve yönetmek isteyen kuruluşlar için uygundur. OpenChain'de instance adı verilen her durum için bir yönetici vardır ve bu yönetici, kayıt defterinin kurallarını tanımlar. Son kullanıcılar bu kurallar doğrultusunda değer alışverişini gerçekleştirirler. Kayıt defterindeki her işlem Bitcoin'de olduğu gibi dijital olarak imzalanmaktadır.

Openchain blokzincir teknolojisi şemsiyesi altında yer almakla birlikte, blok yapısını kullanmadığından tam olarak blokzincir olarak nitelendirilmemektedir. Openchain'de işlemler doğrudan birbirlerine zincirlenirler ve bloklar halinde gruplanmazlar. Blokzincirdeki blok yapısı işlemlerde gecikmeye neden olur. En hızlı sistemlerde birkaç saniyelik bir gecikmeyle işlemler tamamlansa bile ticaret gibi gecikmenin çok önemli olduğu uygulamalarda birkaç saniye bile önemli olabilmektedir. Openchain'de işlemler ağa gönderilir gönderilmez zincire bağlanır ve gerçek zamanlı olarak işlem onayı sağlanabilir. Openchain için blokzincir yerine işlem zinciri ifadesini kullanmak daha doğrudur. OpenChain platformunun özellikleri Çizelge 2.15'te verilmiştir.

Çizelge 2.15. OpenChain blokzincir platformunun özellikleri

OpenChain (OpenChain Project, 2016)	
Teknik özellikler	
Ağa katılım	Anonim olarak katılınabilen tamamen açık defter, katılımcıların yönetici tarafından onaylanması gereken özel bir yapı ya da onaylı kullanıcıların anonim kullanıcılardan daha fazla yetkiye sahip olduğu karma bir yapıda olabilir. • Her iki tipte de konfigüre edilebilir (3)
Blokzincir tipi (açık, özel)	Her iki tipte de konfigüre edilebilir (3)
Hash fonksiyonu	İşlemler için SHA256 kullanılmaktadır. Cüzdan adresleri ise açık anahtarların Keccak256 ile hashlenmesi ile elde edilmektedir.
Mutabakat mekanizması	Bitcoin'de kullanılan fikir birliği mekanizmasının aksine, bir örneğin işlemlerin doğrulanması için yalnızca tek bir yetkiye sahip olduğu Partionned Consensus kullanır. Şifreli anahtarları kaba kuvvet (brute force) saldırısına karşı daha dirençli hale getirmek için PBKDF2, anahtar türetmek için HMACSHA512 ve RIPEMD160 ile SHA256'nın bir kombinasyonu olan RIPEMD160SHA256 kullanılmaktadır.

Yazılım dili	Yazılım dili olarak C#, JavaScript, HTML ve Nginx kullanılmaktadır.
Yazılım tipi	Açık kaynak kodludur. https://github.com/openchain adresinde paylaşılmaktadır.
Performans özellikleri	
İşlem hacmi	Özel ve izin gerektiren ağ için işlem hacmi çok yüksek olarak değerlendirilmektedir.
Ağ gecikmesi	İşlemler anlık olarak gerçekleşmektedir.
Ölçeklenebilirlik (side-chain, sharding, plasma-chain, off-chain)	Blok yapısı yerine işlem zincirleri biçimindeki yapısı Openchain ağını daha ölçeklenebilir ve sağlam kılmaktadır. • Yüksek (3)
İşlem hızı	İşlemler anlık olarak tamamlanmaktadır. Çok hızlı olarak değerlendirilmektedir.
Blokzincir üçlü çelişkisi	Yapılan tasarıma göre değişkenlik göstermekle birlikte, özel ve izin gerektiren bir tasarımda merkezsizlikten taviz verilmektedir. • Ölçeklenebilir ve güvenli ama merkezi (1)
Güvenliğe ilişkin özellikler	
DoS ve DDoS saldırılarına direnç	Özel ve izin gerektiren tasarımı DDoS saldırılarına karşı dirençlidir. Yüksek (3)
Sybil saldırısına direnç	Openchain ağına saldırının gerçekleştirilmesi mantıklı değildir. Birden fazla hesap oluşturmak, cüzdanın ağırlığı ve güvenilirliği ağı etkileyeceği için fayda sağlamayacaktır. Bu nedenle Sybil saldırısına karşı direnci "yüksek" (3) olarak değerlendirilmektedir.
Kuantum bilişim riskine direnç	Bitcoin ile aynı derecede dirençlidir. • Yüksek (3)
Mahremiyet ve gizlilik teknolojisi	Multisignature (çoklu imza) kullanılmaktadır. Çoklu imzalı bir şemada, bir grup kullanıcı tek bir mesajı imzalar. Bir blokzincir ağında, bir işlem bir grup katılımcının imzasını gerektirdiğinde, çoklu imza şeması kullanmak avantajlı olabilir. Openchain ve MultiChain gibi platformlar, M-1 kriptografik anahtarların uzlaşmasını tolore ederek hırsızlık riskini azaltan $M - of - N$ çoklu imza şemasını destekler (Raikwar, Gligoroski ve Kralevska, 2019). • Yüksek (3)
Kullanım amacına ilişkin özellikler	
Uygulama türü	OpenChain, dijital varlıkları güvenli ve ölçeklenebilir bir şekilde yönetmek için çok uygundur. Genellikle bir sahiplik kaydı olarak kullanılır. Hisse senetleri ve tahviller gibi menkul kıymetler, altın ve petrol gibi emtialar, Dolar ve hatta Bitcoin gibi para birimleri, arazi tapuları, müzik veya yazılım lisanslama gibi mülkiyet başlıkları, hediye kartları ve bağlılık puanları başlıca kullanım alanlarıdır. • Genel amaçlı (1)
Akıllı sözleşme desteği	• Evet (1)
Akıllı sözleşme dil desteği	Tüm JVM dilleri (Java, Clojure, Groovy, Kotlin, Scala vb.). Akıllı sözleşmelerde kullanılmasına izin verilen sınıf ve yöntem sayısı sınırlıdır. Primitives, diziler, ArrayList, HashSet, HashMap ve StrictMath kullanımına izin verilir.
Token kullanımı	• Evet (1)
Niteliksel özellikler	
Olgunluk	2015 yılında kurulmuş olup nispeten eski olmasına karşın projeye yapılan son kod taahhüdünün tarihinin 2017 olması nedeniyle olgunluğu orta-düşük olarak nitelendirilmektedir. • Orta (3)
Pazardaki popülarite	Openchain, 14 Platinum üyesi tarafından birçok farklı projede uygulanmıştır. En iyi bilinenleri GitHub, Adobe, Hitachi, Toyota, Sony ve Qualcomm'dur. Ancak diğer platformlara kıyasla Openchain geliştirici topluluğu çok aktif değildir. GitHub'daki projeye yapılan son kod taahhüdü 2017 yılına aittir. Bu nedenle popülaritesi orta-düşük olarak değerlendirilmektedir. • Orta (3)
Geliştirici	Coinprism firması tarafından geliştirilmiştir.
Güvenilirlik	Olgunluk, popülarite ve geliştirici özellikleri dikkate alınarak "düşük" (2) olarak değerlendirilmektedir.

- BigchainDB

BigchainDB hem merkezsizlik, değiştirilemezlik, sahibi tarafından kontrol edilen varlıklar gibi blokzincir özelliklerine, hem de yüksek işlem hızı, düşük gecikme süresi, yapılandırılmış verilerin indekslenmesi ve sorgulanması gibi veritabanı özelliklerine sahip bir blokzincir platformudur. Açık kaynak kodlu olarak 2016 yılı Şubat ayında piyasaya sürülmüştür. Birçok kullanım senaryosu için kullanılabilirdir (BigchainDB GmbH, 2018).

BigchainDB geleneksel blokzincir ile dağıtık veritabanlarının temel avantajlarını bir araya getirmektedir. Bunun için kurumsal düzeyde dağıtık bir veritabanı olan MongoDB ile kullanıma hazır bir mutabakat motoru olan Tendermint'i kullanmaktadır.

Tendermint, bir uygulamayı birçok makinede güvenli ve tutarlı bir şekilde çoğaltmak için kullanılan bir yazılımdır. Tendermint iki ana teknik bileşenden oluşur: bir blokzincir konsensüs motoru ve genel bir uygulama arayüzü. Tendermint Core adı verilen konsensüs motoru, aynı işlemlerin her makinede aynı sırada kaydedilmesini sağlar. Uygulama Blok Zinciri Arayüzü (ABCI) olarak adlandırılan uygulama arayüzü, işlemlerin herhangi bir programlama dilinde işlenmesini sağlar (Tendermint Inc., tarih yok).

BigchainDB verileri varlık olarak yapılandırmaktadır. Her şeyin bir varlık olarak temsil edilebileceği fikrinden hareketle BigchainDB'deki verinin temsil ettiği varlık bir otomobil, belge, telif hakkı, bir makinanın çalışma durumu, kullanıcı izni ya da yaratılan herhangi bir token olabilmektedir. Sürece değil varlığa odaklanılır. Varlıklar "Create" ve "Transfer" olmak üzere iki biçimde kaydedilir. Bu varlıklar fiziksel ya da dijital bir nesne olabilir. BigchainDB blokzincir platformunun özellikleri Çizelge 2.16'da verilmiştir.

Çizelge 2.16. BigchainDB blokzincir platformunun özellikleri

BigchainDB	
Teknik özellikler	
Ağa katılım	Ağ içerisinde farklı kullanıcı tipleri tanımlanarak farklı izinler verilebilmektedir. • Her iki tipte de konfigüre edilebilir (3)
Blokzincir tipi (açık, özel)	Spesifik kullanım durumuna göre açık ya da özel olarak tasarlanabilmektedir. • Her iki tipte de konfigüre edilebilir (3)
Hash fonksiyonu	İşlem ve blok hash değerleri için SHA3-256 (Keccak) kullanılmaktadır.
Mutabakat mekanizması	Tüm ağ ve mutabakat işlemleri için Tendermint kullanılmaktadır. Ağdaki her düğüm kendi lokal MongoBD veritabanına sahiptir. Ağdaki düğümler arasındaki iletişim Tendermint protokolleriyle sağlanır. Tendermint'in de sahip olduğu gibi

	BigchainDB BFT (Bizanslı Hata Toleransı) özelliğine sahiptir. Yani, ağdaki düğümlerin üçte biri kötü niyetli ya da hatalı olsa bile ağ uygun biçimde mutabakat sağlayabilmektedir.
Yazılım dili	https://github.com/bigchaindb/bigchaindb adresinden alınan verilere göre kullanılan yazılım dilleri Python (%83,5), Shell (%13), Lua (%1,6), Dockerfile (%0,8), Makefile (%0,6), HTML (%0,3) ve JavaScript (%0,2) biçimindedir.
Yazılım tipi	Açık kaynak kodludur.
Performans özellikleri	
İşlem hacmi	Saniyede 636 işlem gerçekleştirilebilmektedir.
Ağ gecikmesi	Çok düşüktür (1).
Ölçeklenebilirlik (side-chain, sharding, plasma-chain, off-chain)	BigchainDB, veri deposu olarak dâhili olarak RethinkDB'yi kullanır. Bu, RethinkDB uygun şekilde yapılandırıldığında BigchainDB'yi ölçeklenebilir hale getirmektedir. • Yüksek (3)
İşlem hızı	765 byte boyutundaki işlemlerle 4 düğümlü bir sistemde yapılan testlerde bir milyon işlem 26 dakikada gerçekleştirilmiş, işlemlerin %99,7'si 2,033 saniyede, %95'i 0,113 saniye içinde, %68'i de 0,018 saniye içinde tamamlanmıştır. Sistem ortalama olarak saniyede 636 işlem gerçekleştirmiştir.
Blokzincir üçlü çelişkisi	Ölçeklenebilirlik ve güvenlik üst düzeyde sağlanmakla birlikte genellikle özel bir blokzincir olduğundan merkezsizlik özelliğinden ödün verilmektedir. • Ölçeklenebilir ve güvenli ama merkezi (1)
Güvenliğe ilişkin özellikler	
DoS ve DDoS saldırılarına direnç	NGINX or HAProxy gibi ters proxy ile gelen http istekleri BigchainDB sunucusundan önce karşılanacak biçimde tasarım yapılabilmektedir. Maksimum işlem boyutu sınırlandırılabilmektedir. • Yüksek (3)
Sybil saldırısına direnç	Bitcoin'de Sybil saldırısı saldırıyı çok maliyetli hale getirerek engellenmektedir. BigchainDB'de ise Sybil saldırısı ağdaki yönetici tarafından üye listesinin tutulması ile önlenir. Dolayısı ile Sybil saldırısına dirençlidir. • Yüksek (3)
Kuantum bilişim riskine direnç	Kullanılan SHA3-256 şifreleme kuantum bilişime dirençlidir. • Yüksek (3)
Mahremiyet ve gizlilik teknolojisi	Farklı kullanıcı tipleri tanımlanarak farklı izinler verilebilmektedir. BigchainDB, MongoDB ve Tendermint tarafından bir düğümde depolanan tüm verilerin şifrelenmesi bir hizmet olarak sağlanabilmektedir.
Kullanım amacına ilişkin özellikler	
Uygulama türü	BigchainDB, merkezsiz, değiştirilemeyen ve veritabanında depolanan her şeyi bir varlık olarak işleme yeteneği gibi blokzincir özelliklerine sahip sorgulanabilir bir veritabanı arayan geliştiriciler ve kuruluşlar için geliştirilmiştir. Performans gereksinimi duyulan büyük hacimli veriler için kullanımı uygundur. Bazı kullanım örnekleri telif hakları (Resonance adlı müzik yapımcı ve dinleyicilerine yönelik müzik yayın birliği), dijital kimlik (Recrui adlı insan kaynakları uygulaması), tedarik zinciri (innogy adlı firma tarafından yürütülen Dijital Ürün Belleği projesi), Kamu hizmetleri (Gana'da tapu kaydı uygulaması olan BenBen projesi) biçimindedir. • Genel amaçlı (1)
Akıllı sözleşme desteği	Herhangi bir akıllı sözleşmenin (yani bir bilgisayar programının) kaynak kodu BigchainDB'de saklanabilir, ancak BigchainDB keyfi akıllı sözleşmeleri çalıştırmamaktadır. BigchainDB, "basit sözleşmeler" olarak adlandırılan "kripto koşulları" kullanılarak ifade edilebilen akıllı sözleşmelerin alt kümesini çalıştırmaktadır. Bir varlığın sahipleri, varlığın yeni sahiplere devredilmesi için yerine getirilmesi gereken koşulları empoze edebilir. Bu koşullar döngüleri veya özyinelemeyi içeremez. • Evet (1)
Akıllı sözleşme dil desteği	"Kripto koşulları" Phyton ve JavaScript başta olmak üzere BigchainDB'de kullanılan dillerle oluşturulabilmektedir.

Token kullanımı	Token yaratılmasını desteklemektedir. BigchainDB'de token bölünebilir bir varlık olarak temsil edilebilmektedir. Bölünebilir varlık kendisine bağlı sabit sayıda alt varlığa sahip bir varlıktır. • Evet (1)
Niteliksel özellikler	
Olgunluk	İlk olarak 2013 yılında geliştilmeye başlayan projenin beta sürümü 2014 yılında yayınlanmış, 2015 yılında da Bitcoin blokzincir platformuna dayalı ilk sürümü piyasa sürülmüştür. Daha sonra, 2015 yılında MongoDB kullanan BigchainDB çalışmalarına başlanmış, 2016 yılında bu sürüm duyurulmuştur. Olgunluk düzeyi "yüksek" (4) olarak değerlendirilmektedir.
Pazardaki popülarite	Klasik blokzincir platformlarına göre hız ve yüksek işlem hacmi özellikleri, veritabanı yapısı ve veri sorgulama özelliği ile gerçek dünya uygulamalarında kullanımı nedenleriyle orta-yüksek olarak değerlendirilmektedir. • Orta (3)
Geliştirici	BigchainDB GmbH adlı firma tarafından geliştirilmiştir.
Güvenilirlik	Olgunluk, popülarite ve geliştirici özellikleri dikkate alınarak "orta" (3) olarak değerlendirilmektedir.

- IOTA

IOTA, insanlar ve makineler arasında değer ve veri alışverişi için bir ağ olan "Her Şeyin İnterneti" için oluşturulmuş ilk dağıtık kayıt defterdir. Platformda blok ve madenci bulunmamakta, işlem gerçekleştirmek için algoritma tarafından belirlenen önceki diğer iki işlemin doğrulanması zorunluluğuna dayalı bir mekanizma kullanılarak maliyet ve ölçeklenebilirlik sorununun üstesinden gelinmektedir.

Platform ilk defa 2015 yılında duyurulmuş olup madenciliğin merkezileşmesi, düşük ağ hızı, ölçeklenebilirlik ve işlem hacmi sorunlarını çözmek için Tangle adı verilen yeni bir yapı kullanılmıştır. Tangle sıralı olmayan düğümlerden oluşan bir sistem olan Directed Acyclic Graph (DAG) kullanmaktadır. DAG veri yapısı diğer blokzincir platformlarından farklı olarak işlemlerin paralel olarak eklenmesine izin vermektedir. Bu nedenle ölçeklenebilirlik sorunu yoktur. Sensörler gibi cihazlar için tasarlanmıştır ve kaynak gereksinimi çok düşüktür. İşlemler tamamen ücretsizdir. 1 sent ya da 1 milyon dolar para transferi de aynı biçimde, hızda ve sıfır ücretle gerçekleştirilebilmektedir. IOTA işlemleri birkaç dakika içinde onaylanmaktadır. Kullanılan Winternitz imzaları kuantum bilişime karşı dirençlidir.

IOTA ağları, aynı düğüm yazılımını çalıştıran birbirine bağlı düğümlerden oluşur. Bu yazılım, düğümlerin Tangle'a okuma/yazma erişimini sağlar, işlemleri doğrulamalarına ve işlemleri yerel defterlerinde saklamalarına izin verir.

IOTA genellikle düşük kapasiteli, sınırlı depolama alanına sahip düğümler için tasarlanmıştır ve işlemler bu nedenle bu düğümlerin veritabanlarını hızla doldurabilmektedir. Bu, IOTA'nın düşük seviyeli, kaynak kısıtlı cihazlarla entegrasyon üzerinde çalıştığı Nesnelerin İnterneti için bir sorun teşkil etmektedir. Bu nedenle, düğüm sahiplerinin eski işlemleri silmesine ve Tangle veritabanlarını küçük tutmalarına olanak tanıyan yerel anlık görüntüleri (snapshots) kullanıma sunulmuştur. Ancak; birçok kullanım senaryosu için verilerin daha uzun süreler saklanması gerekmektedir. Örneğin, finansal verilerin bazı durumlarda 10 yıl, kimlik verilerinin ise kimliğin ömrü boyunca saklanması gerekmektedir. Bu tip durumlarda IOTA'nın kullanılabilmesi için "Permanode" adı verilen yapı üzerinde çalışılmaktadır (IOTA, tarih yok).

Permanode adı verilen bu yapı için geliştirilen çözüm ise Chronicle olarak adlandırılmaktadır. Chronicle düğüm sahiplerinin tüm IOTA işlemlerini hızlı, güvenli, ölçeklenebilir ve dağıtık bir veritabanında depolamasını kolaylaştırmakta, Tangle'ın sınırsız veri akışını depolamak ve sorgulanabilir hale getirmek için kullanılmaktadır.

IOTA teknolojisi birçok alanda kullanım için uygundur. Otomotiv başta olmak üzere küresel ticaret, tedarik zinciri, endüstriyel IoT, elektronik sağlık, akıllı şehirler, gümrük ve sınır yönetimi, dijital kimlik uygulandığı başlıca sektörlerdir. IOTA Tangle platformunun özellikleri Çizelge 2.17'de verilmiştir.

Çizelge 2.17. IOTA Tangle platformunun özellikleri

IOTA (IOTA, tarih yok)**,** (Popov, 2018)	
Teknik özellikler	
Ağa katılım	İzin gerektirmeyen ve izin gerektiren olarak tasarlanabilmektedir. • Her iki tipte de konfigüre edilebilir (3)
Blokzincir tipi (açık, özel)	Açık ve özel olarak tasarlanabilmektedir. • Her iki tipte de konfigüre edilebilir (3)
Hash fonksiyonu	Kullanıcıların ödemelerinin onaylanmasında Winternitz One-Time Signatures'a dayalı olan, ancak klasik Winternitz'den farklı olarak mesajın hash değerinin imzalandığı IOTA İmza Şeması (ISS – IOTA Signature Scheme) kullanılmaktadır. ISS'nin dayandığı kriptografik hash fonksiyonu olarak başlangıçta Curl-P-27 kullanılmıştır. Ancak bazı güvenlik zafiyetlerinin ortaya çıkmasıyla 2017 yılı Ekim ayından sonra Keccak'a dayalı bir hash fonksiyonu olan Kerl kullanılmaya başlanmıştır (Heilman, ve diğerleri, 2020). Chrysalis ve Coordicide sürümleri ile de Ed25519 (Edwards-curve Digital Signature Algorithm - EdDSA) kullanılmaya başlanmıştır.
Mutabakat mekanizması	Koordinatör adı verilen, IOTA Vakfı tarafından yönetilen düğümün işlem onayına dayalı mutabakat mekanizmasının Coordicide ile değiştirilmesi ile Hızlı Olasılıksal Mutabakat (FPC – Fast Probabilistic Consensus) ve Hücresel Mutabakat (CC – Cellular Consensus) kullanılmaktadır. Temelinde oy çokluğuna

	dayanan bu mutabakat mekanizmasında her düğüm rastgele seçilen k adet düğümü sorgulayarak kendi fikrini bu sorguladığı düğümlerin çoğunluğuna göre belirlemektedir (Popov, ve diğerleri, 2020).
Yazılım dili	https://github.com/iotaledger adresinden alınan verilere göre kullanılan yazılım dilleri JavaScript, Java, Rust, TypeScript ve C'dir.
Yazılım tipi	Açık kaynak kodludur.
Performans özellikleri	
İşlem hacmi	27 Temmuz 2020'deki Pollen güncellemesi ile saniyede maksimum 10 bin işlem hızına erişilmiştir.
Ağ gecikmesi	İşlemler 10 – 12 saniyede sonuçlanmaktadır. Ağ gecikmesi çok düşüktür.
Ölçeklenebilirlik (side-chain, sharding, plasma-chain, off-chain)	Kullanılan Directed Acyclic Graph (DAG) veri yapısı diğer blokzincir platformlarından farklı olarak işlemlerin paralel olarak eklenmesine izin vermektedir. Bu nedenle ölçeklenebilirlik sorunu yoktur. • Yüksek (3)
İşlem hızı	İşlem hızı yüksektir.
Blokzincir üçlü çelişkisi	IOTA'da kullanılan protokol bir dizi merkezi bileşen kullandığından merkezsizlik özelliğinden feragat etmektedir. Protokoldeki en önemli merkezi bileşen diğer tüm düğümlerin geçeli kabul ettiği kilometre taşı işlemleri düzenli biçimde sağlayan ve Koordinatör adı verilen düğümdür. Merkezi bir sunucu olan Koordinatör işlem güvenliğini sağlamakla birlikte tek nokta hatasına açıktır. Ayrıca, paralel işlemlere izin vermediği için ağ hızını da olumsuz etkilemektedir. Bu nedenle IOTA Vakfı Koordinatör yapısı yerine "Coordicide" adı verilen bir yapı kullanmaya başlamıştır. Coordicide düğüm sahiplerinin tüm IOTA işlemlerini hızlı, güvenli, ölçeklenebilir ve dağıtılmış bir veritabanında depolamasını kolaylaştırmaktadır. • Ölçeklenebilir ve güvenli ama merkezi (1)
Güvenliğe ilişkin özellikler	
DoS ve DDoS saldırılarına direnç	Klasik blokzincir yapısından farklı olan DAG ile DDoS saldırılarına karşı daha dirençlidir. • Yüksek (3)
Sybil saldırısına direnç	Sybil saldırısına karşı dirençlidir. Bu direnç kullanıcıların sahip oldukları itibar değerini gösteren bir token yapısı ile sağlanmaktadır (Popov, ve diğerleri, 2020). • Yüksek (3)
Kuantum bilişim riskine direnç	Halihazırda, Tangle'da depolanan herhangi bir verinin aksine, iletişim katmanında kuantum sonrası kriptografiye gerek duyulmamaktadır. Ancak sistem gelecekte gerekmesi halinde kuantum saldırılarına karşı dirençli kriptografiye geçiş için uygundur (Popov, ve diğerleri, 2020). • Yüksek (3)
Mahremiyet ve gizlilik teknolojisi	Maskelenmiş Kimliği Doğrulanmış Mesajlaşma (MAM - Masked Authenticated Messaging) adı verilen veri iletişim protokolü ile Tangle'daki işlemlerde kanal adı verilen şifreli veri akışları yayınlanır. • Yüksek (3)
Kullanım amacına ilişkin özellikler	
Uygulama türü	İnsanlar ve makineler arasında değer ve veri alışverişi için bir ağ olan "Her Şeyin İnterneti" için oluşturulmuştur. IOTA teknolojisi birçok alanda kullanım için uygundur. Otomotiv, küresel ticaret, tedarik zinciri, endüstriyel IoT, elektronik sağlık, akıllı şehirler, gümrük ve sınır yönetimi, dijital kimlik uygulandığı başlıca sektörlerdir. • Genel amaçlı (1)
Akıllı sözleşme desteği	2021 yılı Mart ayında duyurulmuş olan IOTA Akıllı Sözleşme Protokolü (ISCP) Alpha ile izin gerektiren (permissioned) akıllı sözleşmeleri desteklemektedir.
Akıllı sözleşme dil desteği	Akıllı sözleşme programı temelde Sanal Makine (VM) için talimatlar içeren bir algoritmadır. IOTA akıllı sözleşmeler için ana VM olarak WebAssembly (WASM), akıllı sözleşmeler için VM katmanında Abra adlı bir akıllı sözleşme dili kullanılmaktadır. IOTA Tangle ağında akıllı sözleme mesajlaşma katmanında ise Quorum'a dayalı bir yapı kullanılmaktadır. Bu iki katman arasındaki bağlantı Qubic Hesaplama Modeli (QCM) ile, Qubic projesi kapsamında sağlamaktadır.

Token kullanımı	MIOTA adı verilen token kullanılmaktadır.
Niteliksel özellikler	
Olgunluk	İlk olarak 2015 yılında ortaya çıkmış olup 2020'de Coordicide versiyonu ile yapısal değişikliğe gitmiştir. Halen geliştirme çalışmaları devam ettiğinden olgunluk düzeyi "orta" (3) olarak değerlendirilmektedir.
Pazardaki popülarite	Klasik blokzincir platformlarından farklı yapısı, özellikle otomotiv alanındaki güçlü kullanımı nedenleriyle ve Volkswagen, Bosch gibi firmalarla yaptıkları anlaşmalarla popülaritesi "yüksek" (4) olarak değerlendirilmektedir.
Geliştirici	David Sønstebø, Dominik Schiener, Sergey Ivancheglo, and Serguei Popov tarafından geliştirilmiştir. Başlangıçta kitlesel fonlama ile, katılımcıların IOTA token satın almalarıyla fonlanmış olup 2017'de IOTA Vakfı kurulmuştur.
Güvenilirlik	Olgunluk, popülarite ve geliştirici özellikleri dikkate alınarak "orta" (3) olarak değerlendirilmektedir.

- HydraChain

HydraChain, izin gerektiren dağıtık kayıt defterleri oluşturmak için Ethereum platformunda destek ekleyen, Ethereum platformunun bir uzantısıdır. Birincil uygulama alanı özel ya da konsorsiyum zincirlerinin kurulmasıdır. Ethereum protokolü ve akıllı sözleşmeleri ile %100 uyumludur. Açık kaynak kodlu bir platform olan HydraChain'de doğrulayıcılar olarak adlandırılan düğümlere dayalı bir mutabakat mekanizması kullanılmaktadır. Özel bir blokzincir olan HydraChain bu yapısı ile işlemleri çok hızlı bir biçimde gerçekleştirebilmektedir (Brainbot Technologies, 2016). HydraChain blokzincir platformunun özellikleri Çizelge 2.18'de verilmiştir.

Çizelge 2.18. HydraChain blokzincir platformunun özellikleri

HydraChain (Hydra Chain, 2018)**,**	
Teknik özellikler	
Ağa katılım	İzin gerektiren (1)
Blokzincir tipi (açık, özel)	Özel (2)
Hash fonksiyonu	Ethereum ile aynı altyapıyı kullanmaktadır
Mutabakat mekanizması	Doğrulayıcılar olarak adlandırılan düğümlere dayalı Hisse Ispatı (PoS) protokolü kullanılmaktadır.
Yazılım dili	https://github.com/Hydra-Chain/node adresinden alınan verilere göre kullanılan yazılım dilleri C++ (%74,5), Python (%12,6), C (%5,1), Shell (%3,8), M4 (%1,3), Makefile (%1,1), diğer (%1,6) biçimindedir.
Yazılım tipi	Açık kaynak kodludur.
Performans özellikleri	
İşlem hacmi	Günde 11 milyondan fazla işlem kapasitesine sahiptir (Ethereum'un 10 katı). Saniyede 75-80 işlem gerçekleştirilebilmekte olup bu rakamı 540 işleme kadar artırabilme esnekliğine sahiptir.
Ağ gecikmesi	Ağ gecikmesi yoktur. Onaylayıcı düğümler bloğu imzaladıktan sonra blok zincire eklendiği anda işlem sonlanmış olmaktadır.
Ölçeklenebilirlik (side-chain, sharding, plasma-chain, off-chain)	Ölçeklenebilirlik sorunu yoktur. • Yüksek (3)

İşlem hızı	İşlem hızı Ethereum'a kıyasla yüksek olmakla birlikte diğer platformlarla karşılaştırıldığında "orta" (3) olarak değerlendirilmektedir.
Blokzincir üçlü çelişkisi	Ethereum'un özel ve izin gerektiren yapıda bir uyarlaması olarak merkezsizlik len feragat edilmektedir. • Ölçeklenebilir ve güvenli ama merkezi (1)
Güvenliğe ilişkin özellikler	
DoS ve DDoS saldırılarına direnç	Ethereum ile aynı biçimde, direnci "yüksek" (3) olarak nitelendirilmektedir
Sybil saldırısına direnç	Ethereum ile aynı biçimde, direnci "yüksek" (3) olarak nitelendirilmektedir
Kuantum bilişim riskine direnç	Ethereum ile aynı biçimde, direnci "yüksek" (3) olarak nitelendirilmektedir
Mahremiyet ve gizlilik teknolojisi	Kimlik İspatı (Proof of Identity) adı verilen, KYC/AML uyumlu, sistemdeki tüm işlemlerin yalnızca kayıtlı katılımcılar arasında olmasını sağlayan bir uzantı kullanılmaktadır. Amaç, mahremiyeti olabildiğince korurken tam denetlenebilirliğin sağlanmasıdır. • Yüksek (3)
Kullanım amacına ilişkin özellikler	
Uygulama türü	Ethereum'un güçlü akıllı sözleşme desteğinin özel ve izin gerektiren ağlarda kullanılması gerektiği durumlar için, özellikle finans uygulamaları için uygundur. • Sadece belirli işlemler için (2)
Akıllı sözleşme desteği	Ethereum'un bir uzantısıdır ve akıllı sözleşmeler ve dağıtık uygulamalar (DApps) geliştirmek ve dağıtmak için çok uygundur. HydraChain, Python yüksek seviye dilinde akıllı sözleşmeler geliştirmek için bir altyapı sağlamaktadır. Geliştirme sürelerinin önemli ölçüde azaltılması ve daha iyi hata ayıklama yetenekleri gibi avantajları bulunmaktadır. Ethereum Sanal Makinesi atlandığı için, yerel sözleşmeler çok daha hızlı yürütülmektedir. Yerel Sözleşmeler Solidity veya Serpent dillerinde yazılmış EVM tabanlı sözleşmelerle birlikte çalışabilmekte ve aynı zincirde birlikte var olabilmektedir.
Akıllı sözleşme dil desteği	Python, Solidity, Serpent
Token kullanımı	Ethereum'daki ERC20'ye eşdeğer HRC20 adı verilen token kullanılmaktadır. HRC20 Hydra'daki akıllı sözleşmelerin içerisindeki tokenler için kullanılan standart bir API'dir.
Niteliksel özellikler	
Olgunluk	Hydra Chain'in temelleri 2018 yılında LockTrip projesinin arkasındaki ekibin yayınladığı "LockTrip Blockchain Manifest" başlıklı dokümana dayanmaktadır. Qtum, Ethereum, Blackcoin ve Bitcoin açık kaynaklarına dayanarak geliştirilmiş olup Hydra teknik dokümantasyonu orijinal olarak Qtum Vakfı tarafından dağıtılan dokümanın bir uyarlamasıdır. Diğer platformlara kıyasla daha yakın zamanda ortaya çıkmış olması, henüz geliştirilmeye devam etmesi ve diğer platformlara göre ortaklık ve uygulama sayısının azlığı nedeniyle olgunluğu "düşük" (2) olarak değerlendirilmektedir.
Pazardaki popülarite	"Orta" (3) olarak değerlendirilmektedir.
Geliştirici	Brainbot Technologies ve Ethereum Ventures tarafından geliştirilmiştir.
Güvenilirlik	Olgunluk, popülarite ve geliştirici özellikleri dikkate alınarak "düşük" (2) olarak değerlendirilmektedir.

- Avalanche

Avalanche merkezi olmayan uygulamaları ve kurumsal blokzincir uygulamalarını birlikte çalışabilir, yüksek oranda ölçeklenebilir tek bir ekosistemde çalıştırmak için geliştirilmiş, açık kaynaklı bir platformdur. Saniyede 4 500'den fazla işlemi proses ederek anında onaylayan ilk akıllı sözleşme platformudur. Diğer merkezi olmayan ağlardan temel farkı

mutabakat protokolüdür. Avalanche protokolü merkezsizlikten ödün vermeden güçlü güvenlik, hızlı işlem kesinliği ve yüksek işlem hacmi elde etmek için mutabakatta yeni bir yaklaşım kullanmaktadır.

Avalanche Exchange Chain (X-Chain), Platform Chain (P-Chain) ve Contract Chain (C-Chain) olmak üzere üç yerleşik blokzincire sahiptir. Bu üç blokzincirin tümü Birincil Ağ tarafından doğrulanmakta ve güvence altına alınmaktadır. Birincil ağ özel bir alt ağdır ve tüm özel alt ağların tüm üyeleri, yani düğümler an az 2 000 AVAX (Avalanche platformunun kripto para birimi) teminatla (stake etmek) Birincil Ağın üyesi olmalıdır. Alt ağ bir dizi blokzincirin durumu hakkında mutabakata varmak için birlikte çalışan dinamik bir doğrulayıcılar grubudur. Her blokzincir tam olarak bir alt ağ tarafından doğrulanmaktadır. Bir alt ağ birçok blokzinciri doğrulayabilmekte ve bir düğüm birçok alt ağın üyesi olabilmektedir.

AvaLabs tarafından geliştirilmiş bir diğer platform ise Avalanche teknolojisiyle çalışan, % 100 Ethereum özelliğine sahip Athereum'dur. Athereum'un Ethereum'dan tek farkı mutabakat motorudur. Athereum en uzun zincir iş ispatı yerine Avalanche mutabakat protokolünün hisseye dayalı doğrusal zincir versiyonunu kullanmaktadır.

Avalanche Avalanche ve Snowman olmak üzere iki mutabakat motoru kullanmaktadır. Avalanche verimliliği yüksek, paralelleştirilebilir ve kolay budanabilir bir DAG mutabakat protokolüdür. Snowman ise akıllı sözleşmelere çok uygun, yüksek işlem hacimli, optimize edilmiş bir zincir mutabakat protokolüdür. Bu mutabakat protokolünde ilk olarak kullanıcı tarafından yaratılan işlem mutabakat protokolüne katılan bir düğüm olan doğrulama düğümüne gönderilir. Daha sonra "gossip" protokolü aracılığı ile bu işlem ağdaki diğer düğümlere yayılır. Kullanıcının mükerrer harcama yapması halinde bu işlemlerden birini seçmek ve mükerrer harcamayı önlemek için her sorgulama düğümü rastgele küçük bir düğüm alt kümesi seçerek bu kümedeki düğümlere hangi işlemin geçerli olduğunu sorar. Sorgulama düğümü işlemlerden hangisine dair daha fazla geçerlilik yanıtı alırsa kendi yanıtını o yönde değiştirir. Ağdaki her düğüm tüm mükerrer işlemler üzerinde bir fikir birliği sağlayana kadar bu prosedür tekrarlanır (Sekniqi, Laine, Buttolph ve Sirer, 2020). Avalanche blokzincir platformunun özellikleri Çizelge 2.19'da verilmiştir.

Çizelge 2.19. Avalanche blokzincir platformunun özellikleri

Avalanche (Sekniqi, Laine, Buttolph ve Sirer, 2020)**,** (Yin, Sekniqi, van Renesse ve Sirer, 2020)	
Teknik özellikler	
Ağa katılım	Her iki tipte de konfigüre edilebilir (3)
Blokzincir tipi (açık, özel)	Her iki tipte de konfigüre edilebilir (3)
Hash fonksiyonu	ECDSA (secp256k1), SHA256, riepmd160 ve Keccak kullanılmaktadır.
Mutabakat mekanizması	Hisse İspatı (PoS) kullanılmaktadır. Avalanche'a katılmak isteyen aday düğümler belirlenmiş bir süre için, belirlenmiş miktarda hisselerini ortaya koyarlar. Bu hisseler o periyot boyunca kitlenir ve kullanılamaz.
Yazılım dili	https://github.com/ava-labs adresinden alınan verilere göre kullanılan yazılım dilleri Go, Python, TypeScript, Vue ve Shell biçimindedir.
Yazılım tipi	Açık kaynak kodludur.
Performans özellikleri	
İşlem hacmi	CPU'ya bağlı olarak saniyede 4 500'den fazla işlem gerçekleştirilmektedir.
Ağ gecikmesi	3 saniyeden daha kısa sürede işlemler sonlanmaktadır.
Ölçeklenebilirlik (side-chain, sharding, plasma-chain, off-chain)	Ölçeklenebilirlik sorunu yoktur. Platformda binlerce ila milyonlarca katılımcı yer alabilir. Protokolde madencilik yoktur, yeşil ve sürdürülebilir bir mutabakat mekanizması kullanmaktadır. Ağa katılmak için özel donanım gerektirmez. • Yüksek (3)
İşlem hızı	İşlem hızı yüksektir.
Blokzincir üçlü çelişkisi	Güvenlik, ölçeklenebilirlik ve merkezsizlik özelliklerinin üçünü birden karşılamaktadır. • Ölçeklenebilir, güvenli ve merkezsiz (4)
Güvenliğe ilişkin özellikler	
DoS ve DDoS saldırılarına direnç	Doğrulama düğümü olmak için teminat olarak kilitlenen hisse (stake) DDoS saldırılarına karşı direnç sağlamaktadır. • Yüksek (3)
Sybil saldırısına direnç	Hisse İspatı mutabakat mekanizması ile Sybil koruması sağlanmaktadır. • Yüksek (3)
Kuantum bilişim riskine direnç	Avalanche ağ modeli, herhangi bir sayıda sanal makineyi etkinleştirebilmekte olup bu nedenle uygun bir dijital imza mekanizmasına sahip, kuantuma dirençli bir sanal makineyi desteklemektedir. Kuantuma dirençli RLWE (Ring Learning With Errors) tabanlı imzalar da dâhil olmak üzere çeşitli dijital imza şemalarının uygulanması beklenmektedir. Kuantum güvenli kriptografik ilkeleri sağlayan yeni bir sanal makine ile sistemi genişletmek kolaydır. Kuantum bilişim riskine karşı dirençli olarak değerlendirilmektedir. • Yüksek (3)
Mahremiyet ve gizlilik teknolojisi	Ağa saldırmak isteyen saldırgan, sistem tasarımcısı tarafından parametrelendirilebilen belirli bir eşiğin altında olduğunda (Bitcoin'de %51 olan) çok güçlü bir güvenlik garantisi sağlanmaktadır. Avalanche sanal makinesinde imza için eliptik eğri kriptografi (secp256k1) kullanılmaktadır. Bitcoin'de olduğu gibi ECDSA açık anahtarlar önce SHA256 ile hashlenmektedir. Daha sonra bu hash değeri riepmd160 ile tekrar hashlenerek 20 bytelık bir adres elde edilmektedir. Avalanche düğümleri Ethereum Sanal Makinelerini de desteklediğinden kriptografik güvenlik için Keccak hash fonksiyonu da kullanılmaktadır. • Yüksek (3)
Kullanım amacına ilişkin özellikler	
Uygulama türü	Üç kullanım durumu hedeflenmektedir: 1- İzin gerektiren (özel) ve izin gerektirmeyen (açık) uygulamaya özgü blokzincirler oluşturma, 2- Yüksek düzeyde ölçeklenebilir ve merkezi olmayan uygulamalar (Dapps) oluşturma ve kullanma,

	3- Özel kurallar, sözleşmeler ve sözleşme ekleri ile karmaşık dijital varlıklar (akıllı varlıklar) oluşturma. Avalanche herkesin başlatabileceği ve kullanabileceği merkezi olmayan varlık ticaretini çok hızlı bir biçimde sağlayan, merkezi olmayan finans (DeFi), finansal varlıklar, ticaret ve diğer benzer işlemler için bir şemsiye platformdur. • Genel amaçlı (1)
Akıllı sözleşme desteği	Ethereum Sanal Makine aracılığı ile akıllı sözleşmeler desteklenmektedir. Akıllı sözleşmeler zincir dışı (off-chain) çalıştırma ve zincirde (on-chain) doğrulama, paralel çalıştırma özelliklerine sahiptir.
Akıllı sözleşme dil desteği	Solidity ve Solidity++ olarak adlandırılan gelişmiş bir versiyonu kullanılmaktadır.
Token kullanımı	Kendi para birimi olan AVAX kullanılmaktadır.
Niteliksel özellikler	
Olgunluk	2018 yılında çalışmalarına başlanmış, 2020 yılında yayınlanan teknik dokümanları ile faaliyete geçmiştir. Diğer platformlara kıyasla daha yeni olması ve halen geliştirme faaliyetinin sürmesi nedeniyle "orta" (3) olarak değerlendirilmektedir.
Pazardaki popülarite	Kripto para piyasasında pazar payı olarak Nisan 2020 itibariyle 38. sırada olması, birçok merkez bankası ile Merkez Bankası Destekli Kripto Para konusunda sürdürmekte olduğu görüşmeler ve blokzincir teknolojisine getirdiği hız, güvenlik, ölçeklenebilirlik ve merkezsizlik özelliklerini aynı anda sağlama özelliği nedenleriyle popülaritesi "yüksek" (4) olarak değerlendirilmektedir.
Geliştirici	New York merkezli Ava Labs tarafından geliştirilmektedir. Emin Gün Sirer ve Kevin Sekniqi tarafından kurulmuş olup bilgisayar bilimi, ekonomi, finans ve hukuk alanlarından birçok uzmandan oluşan geniş bir ekip tarafından geliştirilmekte ve yönetilmektedir.
Güvenilirlik	Olgunluk, popülarite ve geliştirici özellikleri dikkate alınarak "orta" (3) olarak değerlendirilmektedir.

- Parity

Web 3.0 olarak adlandırılan merkezsizleşmiş web için bir blokzincir altyapısını sunmayı hedefleyen Parity, Parity Ethereum, Parity Substrate ve Web3 Vakfı'nın bir projesi olan Polkadot ile çalışmaktadır. Polkadot farklı mutabakat algoritmaları ve kripto varlık ekonomilerine sahip blokzincirlerin (örneğin Bitcoin, Ethereum, ZCash ve herhangi bir banka ağı) birbirleri ile konuşabilmelerini sağlayan bir ağ arayüzüdür.

Polkadot, özelleştirilmiş yan zincirlerin açık blokzincirlerle bağlantı kurmasını sağlayan heterojen bir çok zincirli değişim ve çeviri mimarisidir. Polkadot birkaç özel blokzinciri tek bir birleşik sistem/ağa bağlayan, yeni nesil bir blokzincir protokolüdür. Günümüz blokzincir mimarilerinin ölçeklenebilirlik ve genişletilebilirlik bakımından yaşadıkları problemi kanoniklik ve geçerliliği birbirlerinden ayıran heterojen, çok zincirli bir mimari ile gideren Polkadot bir federasyon içerisinde birlikte çalışan, açık ve kapalı ağların birbirlerine güvenmeden erişebilmelerini sağlayan çok sayıda mutabakat sistemini mümkün kılmaktadır. Polkadot'un temel özellikleri aşağıdaki biçimdedir (Wood, 2016):

- Birlikte çalışabilirliği geliştirme; Tüm farklı blokzincirleri birbirlerine bağlayarak çeşitli ekosistemler arasında birlikte çalışabilirliği teşvik etmektedir.
- Ölçeklenebilirlik; Doğrulayıcı adı verilen düğümlerin standart bir kümesi Polkadot ile birbirlerine bağlanmış birçok blokzincirde işlem yapabilmekte, böylelikle ölçeklenebilirlik üstel olarak artmaktadır.
- İnovasyon; Polkadot kolay bir biçimde özel blokzincir oluşturmaya imkan vermektedir. Bu geliştirme kolaylığı daha fazla geliştiriciyi sisteme katılmaya teşvik etmektedir.
- Çatallanmanın kaldırılması; Polkadot çatallanmaya gerek kalmadan yeni özellikleri entegre etme, hata düzeltme ve sürüm yükseltme özelliğine sahiptir.

Polkadot ağını oluşturan çok sayıdaki blokzincir parachain olarak adlandırılır ve bunlar relaychain adı verilen merkezi bir blokzincir tarafından koordine edilirler. Ayrıca, tüm sistem için güvenliği ve güven gerekmeksizin birlikte çalışabilmeyi sağlayan, büyük ve paylaşılan bir doğrulayıcı havuzuna sahiptir.

Substrate ise kripto para birimleri ve diğer merkezi olmayan sistemler oluşturmak için geliştirilmiş bir çerçevedir. Substrate kolay biçimde web ya da mobil uygulamaları geliştirmek için kullanılan Express'e benzemektedir. Web uygulamalarının geliştirilirken kendi http versiyonlarını yeniden geliştirmemelerine benzer biçimde, yeni bir blokzincir oluşturan her ekibin tüm ağ iletişimi ve mutabakat kodunu sıfırdan uygulamak zorunda kalmamasını hedeflemektedir. Substrate kullanarak yeni bir proje oluşturmak için kodda çok az düzenleme gerekmekte olup platform ile ücretsiz olarak aşağıdakiler elde edilmektedir (Fransham, 2018):

- Bizanslı hata toleransına sahip bir mutabakat, işlem kesinliği ve blok oylama mantığı,
- Ağ oluşturma, eş keşfi ve replikasyon,
- Diğer Substrate'e dayalı projeleri ya da akıllı sözleşmeleri çalıştırmak için verimli, deterministik ve korumalı WebAssembly çalışma zamanı,
- Herhangi bir masaüstü veya bulut düğümüyle iletişim kurabilen bir düğümü sorunsuz bir şekilde tarayıcıda çalıştırma yeteneği,
- Tarayıcıda bile çalışabilen, platformlar arası veri tabanı/depolama,
- Mutabakatı etkileyebilecek herhangi bir güncelleme ya da kodu WebAssembly içinde derleyerek ve ağdaki başka bir mesaj olarak dağıtmak suretiyle gerçekleştirilen sorunsuz istemci güncellemeleri,

- Proje yayınlandığı anda Polkadot'ta çalıştırılmaya başlama kabiliyeti.

Burada, Polkadot daha çok diğer blokzincir platformlarını birbirlerine bağlamak için kullanıldığından, blokzincir uygulaması geliştirme platformu olan Substrate'in özelliklerine yer verilmiş olup bu özellikler aşağıda, Çizelge 2.20'de sunulmuştur.

Çizelge 2.20. Parity Substrate blokzincir platformunun özellikleri

Parity (Substrate) (Forbes, 2021)	
Teknik özellikler	
Ağa katılım	Her iki tipte de konfigüre edilebilir (3)
Blokzincir tipi (açık, özel)	Her iki tipte de konfigüre edilebilir (3)
Hash fonksiyonu	Kimlik doğrulama için Edwards-Curve Ed25519, hash fonksiyonu olarak Blake2b kullanılmaktadır.
Mutabakat mekanizması	Hibrit PBFT/Aurand kullanılmakta olup Aura (Round Robin), BABE (slota dayalı), GRANDPA ve İş İspatı mutabakat protokolleri ile kendi uygulamasını geliştirmeyi desteklemektedir. Bunun dışında, Substrate ile uygulama geliştirilirken geliştiriciler kendi mutabakat algoritmalarını kullanmakta özgüdür.
Yazılım dili	https://github.com/paritytech/substrate adresinden alınan verilere göre (Ekim 2022) Rust (%98,4), WebAssembly (%1,3), Shell (%0,23), Handlebars (%0,1), Dockerfile ve EJS kullanılmaktadır.
Yazılım tipi	Açık kaynak kodludur.
Performans özellikleri	
İşlem hacmi	Farklı mutabakat algoritmaları ve blokzincir tiplerine sahip blokzincir tasarımı yapma imkânı sağladığından işlem hacmi kullanıcı tasarımına göre değişmekte olup kullanım amacına ve ihtiyaca göre işlem hacmini sağlama kapasitesi bulunmaktadır. Bu nedenle "çok yüksek" olarak değerlendirilmektedir.
Ağ gecikmesi	Farklı tasarımlar yapılabildiğinden standart bir gecikme değeri bulunmamaktadır. Bu nedenle "orta" (3) olarak değerlendirilmektedir.
Ölçeklenebilirlik (side-chain, sharding, plasma-chain, off-chain)	Ölçeklenebilirlik sorunu bulunmamaktadır. Ölçeklenebilirlik özelliği aranan blokzincir çözümlerine uygun tasarım yapmaya elverişlidir. • Yüksek (3)
İşlem hızı	İşlem hızı yüksektir. GRANDPA neredeyse anında blok kesinliği sağlar, BABE ise 6 saniyede bir blok üretmektedir. Saniyede 15 bin işlem gerçekleştirilebilmektedir.
Blokzincir üçlü çelişkisi	Güvenlik ve ölçeklenebilirliği yüksektir. Ancak yapısındaki koordinatör blokzincir ve doğrulayıcılar nedeni ile merkezsisleşmişlik nispeten düşüktür. • Ölçeklenebilir ve güvenli ama merkezi (1)
Güvenliğe ilişkin özellikler	
DoS ve DDoS saldırılarına direnç	Polkadex yapısı işlem ücreti gerektirmemektedir. İşlem ücretinin sıfır olması ile bağlantılı DDoS saldırısı riski ise DDoS saldırısı olabilecek saldırı işlemlerini ücretlendirerek giderilmektedir. Polkadex her işlemi "iyi" ve "potansiyel DDoS saldırısı" olarak sınıflandırmaktadır. Geçersiz fiyat/miktar, yetersiz bakiye, geçersiz işlem çifti ve geçersiz sipariş türü içeren işlemler potansiyel DDoS saldırısı olarak sınıflandırılır. DDoS saldırılarına karşı dirençli olarak değerlendirilmektedir. • Yüksek (3)
Sybil saldırısına direnç	1.8.0 versiyonu ile birlikte Sybil saldırısına karşı dirençli hale gelmiştir. • Yüksek (3)
Kuantum bilişim riskine direnç	Hash fonksiyonu olarak kullanılan BLAKE2b kuantum bilişime karşı dirençlidir. • Yüksek (3)

Mahremiyet ve gizlilik teknolojisi	Kullanım alanına uygun mahremiyet özelliğine sahip blokzincir tasarımı konusunda esnektir. • Yüksek (3)
Kullanım amacına ilişkin özellikler	
Uygulama türü	Substrate kripto para birimleri ve diğer merkezi olmayan sistemler oluşturmak için geliştirilmiş bir çerçevedir. Her amaca yönelik blokzincir tasarımı kolaylıkla yapılabilmektedir. Polkadot, herhangi bir veri veya varlık türünün ağlar arasında aktarımını kolaylaştırır, çeşitli blokzincir yapılarını birlikte çalışabilir hale getirir. • Genel amaçlı (1)
Akıllı sözleşme desteği	Ethereum Sanal Makine aracılığı ile akıllı sözleşmeler desteklenmektedir.
Akıllı sözleşme dil desteği	Rust'a dayalı "ink!" adı verilen gömülü domain spesifik dil kullanılmaktadır.
Token kullanımı	Substrate'e eklenecek bir kütüphane ile token yaratmak ve bu tokenları Hisse İspatı algoritmasında kullanmak mümkündür. Polkadot'un ağ yönetişiminin sağlanması, transfer işlemlerinin gerçekleştirilmesi ve parachain adı verilen paralel zincirlerin oluşturulmasında kullanılan, kriptopara piyasasında Pazar büyüklüğü bakımından ilk on içerisinde yer alan DOT adlı kendi tokeni bulunmaktadır.
Niteliksel özellikler	
Olgunluk	Polkadot teknik dokümanı 2016 yılı Kasım ayında yayınlanmış, ilk token arzı 2017 yılı Ekim ayında tamamlanmıştır. Substrate ise ilk olarak 2018 yılı Ekim ayında, Substrate 2.0 versiyonu ise 2020 yılı Eylül ayında duyurulmuştur. Olgunluğu "düşük" (2) olarak değerlendirilmektedir.
Pazardaki popülarite	Geliştiricisi olan Gavin Wood aynı zamanda Web3 Vakfı başkanı, Ethereum'un kurucularından biri, Solidity dilinin geliştiricisi olup blokzincir ve kriptopara sektörünün en etkili ve tanınmış kişilerinden biridir. 5 Mayıs 2021 itibariyle kriptopara piyasasında pazar payı bakımından sekizinci sıradadır. Popülaritesi "yüksek" (4) olarak değerlendirilmektedir.
Geliştirici	Polkadot İsviçre kaynaklı bir vakıf olan Web3 Vakfı tarafından kurulmuş, Ethereum'un kurucularından Gavin Wood tarafından geliştirilmiştir.
Güvenilirlik	Olgunluk, popülarite ve geliştirici özellikleri dikkate alınarak "orta" (3) olarak değerlendirilmektedir.

- Kadena

Açık bir blokzincir (Chainweb), izin gerektiren bir blokzincir (Kuro) ve Pact akıllı sözleşme dilinden oluşan hibrit bir blokzincir platformudur. Chainweb adı verilen ölçeklenebilir İş İspatına dayalı açık blokzincir ve Kuro adı verilen özel blokzinciri bir arada kullanarak ölçeklenebilirlik sorununa çözüm getirmektedir. Özellikle DeFi sektörüne uygun performans düzeyine sahip ilk İş İspatı algoritması kullanan blokzincir platformudur. Bu performansa sharding adı verilen yöntemle erişilmektedir. Yüksek performanslı, izin gerektiren ağ açık blokzincire bağlanarak birçok kullanım senaryosu için uygun mimariyi sağlamaktadır. Hibrit yapısı ile hem özel hem de açık blokzincirin avantajlarını bir araya getirmektedir. Hem güvenli hem de kullanımı basit olan Pact ile yazılan akıllı sözleşmeler kullanılarak zincirler arası iletişim, çoklu imzalar ve güçlü izin kontrolleri gibi kilit faaliyetler yürütülmektedir. Kadena blokzincir platformunun özellikleri Çizelge 2.21'de verilmiştir.

Çizelge 2.21. Kadena blokzincir platformunun özellikleri.

Kadena (Martino ve Popejoy, 2019), (Martino, Quaintance ve Popejoy, 2018), (Quaintance ve Martino, 2018), (Chitra, Quaintance, Haber ve Martino, 2019), (Martino, 2016), (Popejoy, 2016)	
Teknik özellikler	
Ağa katılım	Her iki tipte de konfigüre edilebilir (3)
Blokzincir tipi (açık, özel)	Her iki tipte de konfigüre edilebilir (3)
Hash fonksiyonu	Hash fonksiyonu olarak Blake2s_256 kullanılmaktadır.
Mutabakat mekanizması	İş İspatı kullanılmaktadır. Ancak geleneksel İş İspatı mutabakat algoritmasının ölçeklenebilirlik sorunu Chainweb adı verilen paralel zincirli yapı ile çözülmüştür.
Yazılım dili	https://github.com/kadena-io/chainweb-node adresinden alınan verilere göre Haskell (%99,2) kullanılmaktadır.
Yazılım tipi	Açık kaynak kodludur.
Performans özellikleri	
İşlem hacmi	Açık Kadena blokzincir platformuda Chainweb yapısı saniyede 10 000 işlem gerçekleştirebilecek en az 1 250 zincir yaratma potansiyeline sahiptir. Özel Kadena blokzincir platformunda ise yapılan denemelerde saniyede 7 000 işleme ulaşılmıştır. Özel blokzincir ağında 5 000 ila 15 000 düğüm arasında performansın kabul edilebilir düzeyde olduğu belirtilmektedir. Kurumsal kullanım için, özel blokzincir ağına katılan her kurumun esnekliği sağlamak adına 3 düğüme ev sahipliği yaptığı varsayılırsa, Kadena ile herhangi bir performans düşüşü yaşanmadan düğüm başına 300 (toplam 900) katılımcıya kadar ağ ölçeklenebilmektedir.
Ağ gecikmesi	Saniyede yaklaşık 7 000 işlem milisaniyeler düzeyinde ağ gecikmesi ile tamamlanabilmektedir.
Ölçeklenebilirlik (side-chain, sharding, plasma-chain, off-chain)	Ölçeklenebilirlik sorunu bulunmamaktadır. Paralelleştirilmiş İş İspatı yapısı ve özel bir sharding çözümü ile ölçeklenebilirlik problemi giderilmiştir. Ağdaki paralel ve birbirinden bağımsız çalışan zincirlerin her biri İş İspatını kullanarak kendi kayıt defterini tutmakta, bu kayıt defterlerinin doğrulanması da Hisse İspatı ile "kuro" olarak adlandırılan firmanın özel zinciri ile yapılmaktadır. • Yüksek (3)
İşlem hızı	Hedef blok zamanı 30 saniyedir.
Blokzincir üçlü çelişkisi	Güvenlik, ölçeklenebilirlik ve merkezsizlik sağlanmaktadır.
Güvenliğe ilişkin özellikler	
DoS ve DDoS saldırılarına direnç	İzin gerektiren blokzincir çözümünü içeren hibrit yapısı ile DDoS saldırılarına karşı direnci "yüksek" (3) olarak değerlendirilmektedir.
Sybil saldırısına direnç	İş İspatı ve Hisse İspatını birlikte kullanan hibrit yapısı ile Sybil saldırısına karşı direnci "yüksek" (3) olarak değerlendirilmektedir.
Kuantum bilişim riskine direnç	Hash fonksiyonu olarak kullanılan BLAKE2b kuantum bilişime karşı dirençli olduğundan direnci "yüksek" (3) olarak değerlendirilmektedir.
Mahremiyet ve gizlilik teknolojisi	Zincir üzerinde şifreleme (on-chain encryption ve Externally-Encrypted Payloads) ile gizlilik sağlanmaktadır. • Yüksek (3)
Kullanım amacına ilişkin özellikler	
Uygulama türü	Özellikle DeFi uygulamaları için hız ve ölçeklenebilirlik sağlamaktadır. Yüksek işlem hacmi, anlık işlemler ve açık ve özel blokzincirin bir arada kullanımı için uygundur. Sigorta, sağlık hizmetleri, finansal hizmetler, tedarik zinciri ve kamu hizmetleri alanlarında müşterileri bulunmaktadır. • Genel amaçlı (1)
Akıllı sözleşme desteği	Desteklenmektedir.
Akıllı sözleşme dil desteği	Pact adlı insanlar tarafından okunabilir yeni bir programlama dili ile akıllı sözleşmeler yazılabilmektedir. Pact akıllı sözleşmeleri tablolar, anahtar setleri ve kod modülü olmak üzere üç temel unsurdan oluşmaktadır.
Token kullanımı	KDA adlı kendi tokeni bulunmaktadır. KDA Kadena ağındaki madencilere madencilik faaliyetleri karşılığında ödül olarak verilmektedir. Ayrıca, kullanıcılar da işlemlerini bir bloğa eklemek için KDA ödemektedir.

Niteliksel özellikler	
Olgunluk	Kadena 2016 yılında kurulmuştur. İlk olarak 2018 yılında Fortune 500 şirketleri tarafından kullanılmaya başlanmıştır. Olgunluğu "orta" (3) olarak değerlendirilmektedir.
Pazardaki popülarite	Geliştiricisi olan Stuart Popejoy ve Will Martino, JP Morgan'ın Blokzincir Mükemmeliyet Merkezi liderliğini yapmış, JP Morgan'dayken, teknolojisi bugünün JPM Coin'ine dönüşen şirketin Juno adlı ilk blok zincirini kurmuşlardır. KDA 10 Mayıs 2021 tarihi itibariyle kriptopara piyasasında 345. sıradadır. Popülaritesi "düşük" (2) olarak değerlendirilmektedir.
Geliştirici	Stuart Popejoy ve Will Martino tarafından kurulmuştur.
Güvenilirlik	Olgunluk, popülarite ve geliştirici özellikleri dikkate alınarak "düşük" (2) olarak değerlendirilmektedir.

- Bir Hizmet Olarak Blokzincir (BaaS) çözümleri

Microsoft Azure BaaS

Bir Hizmet Olarak Blokzincir (blockchain-as-a-service) olarak Microsoft tarafından 2015 yılından itibaren sunulan, kullanıcıların basitleştirilmiş bir blokzincir ağı oluşturma, bu ağı yönetme ve ağı genişletme işlevlerini destekleyen uçtan uca bir platform desteğidir. Geliştirmeyi basitleştirmek ve hızlandırmak için oluşturulmuştur.

Azure, işletmelere blokzincir ağlarını çalıştırma ve büyütme yeteneği sunan, işletmelerin ağ yönetişimi ve altyapısı üzerinde tam kontrol sahibi olduğu bir kayıt defteri sistemidir. Hem süreçleri hem de verileri güvende tutmak için tasarlanmıştır ve şirketlerin güvenle inovasyon yapmalarına olanak tanır.

Blokzincir teknolojisini kullanan uygulamalar geliştirmek konusunda destek vermekle birlikte, bu hizmetleri sunmak için merkezi bir yapı kullanmaktadır. Kapalı bir ekosistemde çalışan, gerçek bir merkezsizlik sağlamayan ancak blokzincirin avantajlarından faydalanmak isteyen kuruluş ve girişimler için idealdir.

Azure bir ön ödeme gerektirmemekte, kullanım durumuna göre düğüm sayısı, depolama alanı gibi faktörler dikkate alınarak periyodik ücretleme yapılmaktadır. Akıllı sözleşme kullanımını desteklemektedir. Microsoft Azure R3 Corda, Hyperledger, Ethereum ve Quorum platformları desteklemekte, açık kaynak kodlu araç desteği sağlamaktadır. Visual Studio kodu Azure blokzinciri destekleyecek biçimde güncellenmiştir.

Tüm işlem ve doğrulayıcı düğümleri güvenlik duvarı kuralları ile korunmakta, tüm işlem düğümleri için TLS ile veri şifreleme sağlanmaktadır. Azure blokzincir uygulamaları ücretsiz olarak sağlanan WorkBench adlı araç ile yönetilmektedir. Bu araç blokzincir uygulamalarının oluşturulması ve dağıtılmasını sağlayan Azure özellikleri ve hizmetlerinden oluşmaktadır. İşlem kuyruk derinliği, çıkarılan bloklar, düğüm depolama, CPU, bellek ve diğer önemli metrikler hakkında önemli bilgiler Azure İzleme Hizmeti tarafından yönetilmektedir.

Özellikle gerçek dünya verilerini, ürün durumlarını izlemek, nakliye risklerini ölçmek ve tedarik zinciri sürecindeki bürokrasiyi azaltarak işlemleri kolaylaştırmak için kullanım örnekleri bulunmaktadır. Tedarik zinciri yönetimi yaygın bir uygulama alanı olsa da kullanım alanı sadece bununla sınırlı değildir. Azure blokzincir platformları hemen hemen her alanda kullanılabilmektedir. Azure blokzincir hizmetini kullanan kuruluşlar arasında Starbucks, Insurwave, Xbox, Nasdaq ve Türkiye'den Migros yer almaktadır.

Azure blokzincir hizmeti blokzincir uygulamaları geliştirmek için çok sayıda araca sahiptir. Bu araçlar ve kullanım alanları aşağıdaki biçimdedir:

Uygulama Hızlandırıcıları:

- Azure Blokzincir WorkBench: Kolayca blokzincir uygulamaları geliştirmeyi sağlar
- Perakende Tedarik Zinciri için Vizix IOT blokzincir: IoT geliştirme aracıdır
- Stratumn Indigo Node: Süreç Kanıtı ağı oluşturmak için bir çerçevedir. Süreç Kanıtı kısaca katılımcıların kimin neyi, ne zaman, hangi sırayl yaptığını değiştirilemez bir şekilde kaydederek ortak bir sürece güvenmesine olanak tanıyan bir protokoldür.
- Ticaret Finansmanı – Akreditif: Ticaret Finansmanı Uygulamasıdır.

Çok Düğümlü Kayıt Defteri:

- Azure'da Ethereum
- Azure'da Quorum
- Azure'da Hyperledger Fabric
- BlockApps Multi-Node Blokzincir: Çoklu özel Ethereum blokzinciri yönetmek için geliştirilmiş kurumsal bir sürümdür.
- EEA Tek Üyeli Blokzincir: Quorum blokzincir ağı yapılandırılarak çalıştırılır.

- Mijin Azure BaaS: Yüksek performans, sıfır kesinti süresi ve yanlışlanamaz verilerle güvenli bir paylaşım ortamı oluşturan özel bir blokzincir platformudur. Mijin, finans kurumları, elektronik para sistemleri, kullanıcı kimlik doğrulaması, arazi ve mülk tescili, lojistik takibi ve gıda izlenebilirliği gibi uygulamalar için idealdir.
- R3 Tek Ağ: Daha önceden yapılandırılmış ağın kullanımına imkân vermektedir.

Araçlar

- Blockctack Core v14: Yeni bir merkezsiz internettir.
- Ethereum Stüdyo – Blokzincir Ortamı: Ethereum blokzincir geliştirme paketidir.
- Truffle: Ethereum geliştirme ortamı, varlık iletişim hattı ve test çerçevesidir.
- Parity Ethereum Dev: Hafif ve hızlı Ethereum kullanımı sağlamaktadır.
- Rewards API: Müşteri sadakat programları ödül çerçevesidir.

Azure blokzincir hizmeti ayrı bir platform olmayıp yukarıda sayılan platformları kullandığından özellikleri için hazırlanmış olan tablo şablonu kullanılmamıştır.

Amazon Managed Blockchain (Hyperledger ve Ethereum)

Açık ağlara kolayca katılmak ya da açık kaynak kodlu Hyperledger Fabric ve Ethereum kullanılarak ölçeklenebilir özel ağlar yaratmak ve bunları yönetmek için kullanılabilen bir hizmettir. Yeni bir blokzincir ağı oluşturmanın karmaşıklığı ve bu ağın yönetiminin güçlüğü gibi sorunlara çözüm getirmek üzere geliştirilmiş, tamamen yönetilen bir blokzincir altyapısıdır. Belirli bir üye grubu içerisinde sıkı gizlilik ve kontrol gerektiren uygulamalara uygun Hyperledger Fabric, şeffaflığın önemli olduğu dağıtık işlemlere uygun Ethereum altyapıları çözüm olarak seçilebilmektedir. Ayrıca, herkese açık bir Ethereum blokzincir ağına katılmak da mümkündür. Önerilen çeşitli CPU ve bellek kombinasyonları ile ölçeklenebilirlik sağlanır. Hyperledger Fabric'te işlem geçmişinin eksiksiz biçimde tutulmamasına karşın Amazon Managed Blockchain blokzincir ağındaki tüm işlemlerin tam geçmişini saklamaktadır.

Amazon Managed Blockchain ön ödeme ya da minimum ücret gerektirmeyen, kullandıkça ödeme yapılan bir fiyatlandırma politikasına sahiptir. Hayperledger Fabric ve Ethereum için

farklı ücretler belirlenmiştir. Amazon Managed Blockchain'in başlıca kullanım alanları ticaret ve varlık transferi, perakende ve tedarik zinciridir.

IBM Blokzincir Platformu

Bir hizmet olarak blokzincir sunan bir diğer servis sağlayıcı IBM'dir. IBM'in Hyperledger'a dayalı çözümleri mevcut blokzincir ağlarından birine katılım, kendi çözümünü oluşturma, IBM ile birlikte blokzincir çözümü oluşturma ve başkaları ile işbirliği yapma biçiminde dört farklı alternatif sunmaktadır.

IBM de diğer servis sağlayıcılar gibi esnek ve kullanıma dayalı bir fiyatlandırma politikasına sahiptir. IBM bulut servisi üzerinden sunulan hizmetler için tahsis Edilen CPU-Saat başına fiyat 0,29$'dır. Bunun dışında, bulut altyapısı için seçim detaylarına göre ücreti değişkenlik gösteren IBM Bulut Kubernetes servis maliyeti, depolama maliyeti ve yedekleme, log kaydı gibi ürün eklentileri de ayrıca ücretlendirilmektedir.

Oldukça yaygın bir kullanıcı portföyüne sahip olan IBM blokzincir hizmeti çözümünün kullanılmakta olduğu başlıca alanlar arasında sağlık hizmetleri, tedarik zinciri, gıda takibi, teminat mektubu, ticaret finansmanı, kimlik yönetimi, eğitim sertifikaları ve elektronik oylama yer almaktadır.

Oracle Blokzincir Bulut Hizmeti

Oracle Blokzincir Bulut Hizmeti akıllı sözleşmelerin oluşturularak kullanılması ve müdahaleye karşı korumalı kayıt defterlerinin tutulması için Hyperledger Fabric'e dayalı bir platform sunmaktadır. Oracle bu hizmet kapsamında dört farklı ürün sunmaktadır:

- Oracle Blokzincir Platformu Bulut Hizmeti: Akıllı sözleşmelerin kullanımına imkan veren, gizli işlemlerin gerçekleştirilmesi, diğer sistemlerle entegrasyon, güvenilir iş ağı ve kapsamlı takip özelliklerine sahip bir üründür.
- Oracle Blokzincir Platformu Kurumsal Sürüm: Daha fazla veri gizliliği gereksinimi duyulan ve yasal düzenlemelerin bulutta çalışmaya izin vermediği koşullar için geliştirilmiş bir çözümdür. Oracle tarafından sunulan özel API'ler ve yönetim araçları sunmakta, OpenLDAP, MS Active Directory ve Oracle Directory ile kimlik yönetimini desteklemektedir.

- Akıllı Takip ve İzleme Sistemi: Tedarik zinciri ağlarında uçtan uca işlemleri, ilişkili varlıkları, ürünlere ilişkin belgeleri takip etmeyi ve denetlemeyi sağlamaktadır. Diğer uygulama yazılımları ve veri kaynaklarına bağlanma, hızlı kurulum ve kullanım ve daha az risk özelliklerine sahiptir.
- Oracle Veritabanı 20c Blokzincir Tabloları: Finansal işlemler, yasal olarak muhafaza edilmesi gereken kayıtlar, denetim logları gibi birçok veri için güvenli bir kayıt defteri çözümüdür.

SAP Leonardo Blockchain Platformu

Diğer SAP uygulamalarıyla entegre olacak biçimde tasarlanmış olan geniş bir kullanım yelpazesine sahip blokzincir platform hizmetidir. Başlıca kullanım alanları arasında tedarik zinciri boyunca ürün ve süreç takibi, süreç kilometre taşlarının otomatik olarak izlenmesi, esnek kriterlere göre eylemlerin tetiklenmesi, sahteciliğin ve yasadışı ticaretin önlenmesi, küresel ve yurtiçi taşımacılığın gerçek zamanlı izlenmesi ve belgelerin gerçek zamanlı olarak birden çok paydaşla paylaşılması yer almaktadır.

SAP Leonardo blokzincir çözümünün SAP Bulut Platformu Blokzinciri ve SAP HANA Blokzicir Hizmeti olmak üzere iki versiyonu bulunmaktadır. Ne SAP Bulut Platformu Blokzinciri ne de SAP HANA, Bitcoin, Ethereum veya Hyperledger Fabric gibi bir blokzincir platformu değildir. SAP'nin blokzincir çözüm stratejisi önerilen ya da ihtiyaç duyulan blokzincir çözümünü mevcut kurumsal blokzincir platformlarına entegre etmektir. SAP Bulut Platformu Blokzinciri şu anda Hyperledger Fabric (SAP aynı zamanda Linux Vakfı Hyperledger projesinin bir üyesidir) ve MultiChain'i desteklemektedir.

Alibaba Bulut Blokzincir Platformu

Alibaba Hizmet Olarak Blokzincir (BaaS) Hyperledger Fabric, Ant Blokzincir ve Quorum'u destekleyen kurumsal düzeyde bir platform hizmetidir. Kullanıma hazır hizmetler sunan, karmaşık yapılandırma gereklilikleri içermeyen hızlı kurulum özelliğine sahiptir. Akıllı sözleşme desteği (chaincode) bulunmaktadır.

Başlıca kullanım senaryoları arasında ürün menşeinin takibi, tedarik zinciri finansı, veri varlıklarının paylaşımı, dijital içerik sahipliği yer almakta olup bu senaryoların hitap ettiği

sektörler perakende, üretim, lojistik, tıp, lüks ürünler, kamu, sigortacılık ve finans olarak belirlenmiştir.

Bunlar dışında Samsung'un Nexledger, Deloitte'in Rubix, Factom'un Harmony adlı bir hizmet olarak blokzincir çözümleri mevcuttur.

2.1.13. Akıllı sözleşmeler

Blokzincir teknolojisinin sağladığı birçok özelliğin içerisindeki en önemlilerinden biri akıllı sözleşmelerdir. Akıllı sözleşme kavramı aslında blokzincir ile birlikte ortaya çıkmış bir kavram değildir. İlk kullanımı çok daha eskilere dayanmaktadır. Bu kavram ilk defa 1996 yılında, bilgisayar bilimci ve programcı Nick Szabo tarafından kullanılmıştır. Szabo (1996) makalesinde bilgisayarların mesaj iletim sistemleri ve algoritmaları bir araya getirerek birçok yeni protokolün geliştirilmesini sağlayacağını belirterek akıllı sözleşmeleri yeni kurumlar ve bu kurumlar arasında yeni ilişkiler oluşturulmasını mümkün kılan dijital bir devrim olarak tanımlamaktadır. Szabo'ya göre akıllı sözleşmeler; dijital olarak belirtilen, birden fazla taraf arasındaki önceden tanımlanmış vaatlerin yerine getirilmesini sağlayan protkolleri içeren kural dizileridir. Akıllı sözleşmelerin temel fikri, birçok farklı sözleşme maddesinin, sözleşme hükümlerini ihlal edecek tarafı engelleyecek ya da ihlalleri maliyetli hale getirecek biçimde yazılım ve donanım içerisine gömülmesidir. Akıllı sözleşmelerin en ilkel örneği para veya jeton ile çalışan otomatlardır.

Akıllı sözleşmeler kripto para dünyasında ilk olarak Vitalik Buterin tarafından geliştirilen, Bitcoin'den sonra kripto para piyasasında değer ve tanınırlık bakımından ikinci sırada bulunan Ethereum ile kullanılmaya başlanmıştır. Buterin (2014), akıllı sözleşmeleri merkezi olmayan otomasyonun en basit formu olduğunu belirterek akıllı sözleşmeleri en doğru ve sade biçimde içerisinde iki ya da daha fazla tarafın ve dijital varlıkların bulunduğu, bu taraflardan bir kısmı ya da tamamının ortaya bir varlık koyarak sözleşmenin başlatıldığı tarihte henüz bilinmeyen belirli bir formülün gerçekleşme durumuna göre bu varlığın yeniden dağıtıldığı bir mekanizma olarak tanımlamaktadır. Yani; akıllı sözleşmelerde anlaşmanın tarafları önce anlaşma maddeleri üzerinde uzlaşarak bunu program kodu haline getirir. Sözleşme içerisinde, sözleşme maddelerinin işlemesini sağlayacak koşullar belirtilir (örneğin 30 takvim günü sonra, alıcı hizmetin tamamlandığını onayladıktan sonra gibi). Bazen bu koşullar dışarıdaki bir sistemden veri alınmasını gerektirebilir. Bu koşullar

karşılandığında, program kodu olarak hazırlanmış olan eylem otomatik olarak gerçekleştirilir. Koşulların karşılanmaması halinde ne olacağı yine program koduna gömülü olarak sisteme dahil edilmiştir. Akıllı sözlemelerin temel özelliği sadece belirli sayıda tarafı içermesidir. Bu tarafların hepsinin sözleşmenin başlatıldığı zamanda biliniyor olması şart değildir. Örneğin; 50 birim A varlığı satmak isteyen A satıcısının 10 birim B varlığı verebilecek herhangi bir alıcıya satışı gerçekleştirmesi de bir akıllı sözleşme örneğidir.

Akıllı sözleşme, yazılı olarak düzenlenmiş olan sözleşmelerin, sözleşme koşullarının gerçekleşip gerçekleşmediğini kendi kendine kontrol ederek doğrulayabilen bilgisayar koduna çevrilmiş halidir. Akıllı sözleşmeler bu kontrol ve doğrulama işleminin ardından, sözleşmede yer alan şarta bağlı hükümlerin de kendi kendine, otomatik olarak yerine getirilmesine izin verir.

Bazı blokzincir platformları küçük bilgisayar programları olan akıllı sözleşmelerin çalıştırılmasını desteklemektedir. Bu programlar belirli şartlar oluştuğunda kendiliklerinden çalışırlar ve doğrudan yazılım koduna gömülmüş sözleşme hükümlerini işletirler. Akıllı sözleşmeler otomatik "eğer/ise" kurallarıdır ve diğer blokzincir işlemleri gibi ağdaki tüm düğümler tarafından işletilirler (Berryhill ve diğerleri, 2018).

Akıllı sözleşmelerin özellikleri kullanıldıkları blokzincirin özel, herkese açık, hibrit ya da zincirler arasında olmasına göre farklılık gösterebilir. Akıllı sözleşmelerin ortaya çıkması blokzincir teknolojisi açısından bir dönüm noktasıdır. Bu nedenle, 2014 yılında Ethereum'un ortaya çıkması ile başlayan dönem Blokzincir 2.0 olarak adlandırılmaktadır.

Wüst ve Gervais (2018) akıllı sözleşmelerin diğer dijital bilgilere ve fiziksel dünyaya ait sistemlere bağlandığında çok daha güçlü hale gelebildiğini ileri sürmektedir. Akıllı sözleşmeler nispeten yeni bir teknoloji olduğundan yasal bağlayıcılıkları ve nasıl yorumlanmaları gerektiği konuları net değildir.

Bir dizi akıllı sözleşme aracılığı ile özerk olarak çalışan organizasyonlar Merkezi Olmayan Otonom Kuruluş (Decentralized Autonomous Organization - DAO) olarak adlandırılmaktadır. Bu organizasyonlarda geleneksel kuruluş ya da şirketlerin aksine merkezi bir kontrol ve yönetim yoktur. Bunun yerine DAO'nun nasıl geliştiğini ve davrandığını tanımlayan akıllı sözleşme kodları bulunmaktadır. Tipik olarak bir DAO'nun

fonlarının nasıl yatırılması gerektiğine oy vererek karar veren birçok yatırımcısı vardır (Wüst ve Gervais, 2018).

2.2. Standardizasyon ve Yasal Düzenleme Çalışmaları

Blokzincir ve dağıtık kayıt defteri teknolojilerindeki hızlı gelişmeler ve ekonomik sektörlerde benimsenmeleri teknik standartlar konusunda titiz bir çalışma yürütülmesi gerekliliğini ortaya çıkarmıştır. Standart mimarilerin kullanılması, dağıtık uygulamalar ve paylaşılan kayıt defterlerinin niteliksel gelişimini sağlaması, standart bir terminolojinin kullanılması etkili iletişimi ve büyümeyi destekleyecektir. Veri standartları teknolojinin düzenlenmesi için bir ön koşul olup birlikte çalışabilirlik, ortak değer üretme ve işbirliği için de çok önemlidir. Benzer biçimde, finansal uygulamalar ile kimlik ve sağlık bilgileri gibi hassas verileri içeren uygulamaların uygun biçimde geliştirilebilmesi için gizlilik ve güvenlik gibi konularda standartlara gereksinim vardır.

Uluslararası düzeyde ve Avrupa bünyesindeki standardizasyon kuruluşlarınca yürütülmekte olan çalışmalar halen devam etmekte olup bunlardan en önemlileri Uluslararası Standardizasyon Teşkilatı (ISO), Uluslararası Telekomünikasyon Birliği (ITU) ve Avrupa Standardizasyon Komitesi (CEN), Avrupa Elektroteknik Standardizasyon Komitesi (CENELEC), Avrupa Telekomünikasyon Standartları Enstitüsü (ETSI) tarafından yürütülen çalışmalardır.

2.2.1. Uluslararası Standardizasyon Teşkilatı (ISO) faaliyetleri

14 Nisan 2016 tarihinde, Avustralya Standartlar Kurumu tarafından blokzincir ve Dağıtık Kayıt Defteri Teknolojileri alanlarında uluslararası standartlar geliştirecek yeni bir ISO Teknik Komitesi (TC) oluşturulması önerilmiş, üye ülkeler arasındaki oylamadan sonra ISO Teknik Yönetim Kurulu 10 Eylül 2016'daki 67. toplantısında teklifi resmen kabul etmiştir. Avustralya, yeni oluşturulan ve ISO/TC 307 olarak adlandırılan bu komitenin sekretarya görevini üstlenmiştir (Standards Australia, 2017).

3 – 5 Nisan 2017 tarihleri arasında Avustralya'da gerçekleştirilen ilk toplantının sonucunda ISO/TC 307 başlığı "Blokzincir ve dağıtık kayıt defteri teknolojileri" kapsamı da "Blokzincir ve dağıtık kayıt defteri teknolojilerinin standardizasyonu" olarak belirlenmiştir.

Yine ilk toplantıda beş araştırma grubu (SG) ve bir çalışma grubu (WG) oluşturulmuş, ihtiyaçlar doğrultusunda daha sonra bu grupların sayısı artırılmıştır. Aşağıda verilmiş olan Çizelge 2.22'de Ekim 2022 itibariyle çalışmaları süren grupların listesi yer almaktadır.

Çizelge 2.22. ISO/TC 307 kapsamında görev yapan araştırma ve çalışma grupları (Ekim 2022)

Referans	Başlık
ISO/TC 307/AG 1	Stratejik İş Planı Gözden Geçirme Danışma Grubu
ISO/TC 307/AG 2	İrtibat Danışma Grubu
ISO/TC 307/AG 3	Dijital para birimleri
ISO/TC 307/AHG 2	Dağıtık Kayıt Defteri Sistemlerinin Denetimi İçin Rehber
ISO/TC 307/AHG 3	Fiziksel varlıkların takas edilemez tokenler (NFT) olarak temsili
ISO/TC 307/CAG 1	Düzenleyiciler Koordinasyon Grubu
ISO/TC 307/JWG 4	Ortak ISO/TC 307 - ISO/IEC JTC 1/SC 27 Çalışma Grubu: Blokzincir ve dağıtık kayıt defter teknolojileri için güvenlik, gizlilik ve kimlik
ISO/TC 307/SG 7	Blokzincir ve dağıtık kayıt defter teknolojilerinin birlikte çalışabilirliği
ISO/TC 307/WG 1	Kuruluşlar
ISO/TC 307/WG 2	Güvenlik, mahremiyet ve kimlik
ISO/TC 307/WG 3	Akıllı sözleşmeler ve uygulamaları
ISO/TC 307/WG 5	Yönetişim
ISO/TC 307/WG 6	Kullanım senaryoları
ISO/TC 307/WG 7	Birlikte çalışabilirlik

Avustralya öncülüğünde 30 katılımcı, 12 gözlemci üye ile başlayan ISO/TC 307 çalışmaları 2022 yılı Ekim ayı itibariyle 42 katılımcı, 21 gözlemci üye ile çalışmalarına devam etmektedir. Bu çalışmalar kapsamında sekiz ISO standardı yayınlanmıştır. Sekiz standart ise henüz geliştirme aşamasındadır. Yayınlanmış olan standartların listesi Çizelge 2.23'te, geliştirilme aşamasında olan standartlar ise Çizelge 2.24'te verilmiştir (ISO, 2022).

Çizelge 2.23. ISO/TC 307 sorumluluğunda yayınlanmış olan standartlar

Standart No	Standart başlığı
ISO 22739:2020	Blokzincir ve dağıtık kayıt defteri teknolojileri - Sözlük
ISO/TR 23244:2020	Blokzincir ve dağıtık kayıt defteri teknolojileri – Mahremiyet ve Kişisel Olarak Tanımlanabilir Bilgileri (PII) koruma hususları
ISO/TR 23249:2022	Blokzincir ve dağıtık kayıt defteri teknolojileri – Kimlik yönetimi için mevcut DLT sistemlerine genel bakış
ISO 23257:2022	Blokzincir ve dağıtık kayıt defteri teknolojileri – Referans mimari
ISO/TS 23258:2021	Blokzincir ve dağıtık kayıt defteri teknolojileri – Taksonomi ve ontoloji
ISO/TR 23455:2019	Blokzincir ve dağıtık kayıt defteri teknolojileri - Blokzincir ve dağıtık kayıt defteri teknolojisi sistemlerindeki akıllı sözleşmelere genel bakış ve bunlar arasındaki etkileşimler
ISO/TR 23576:2020	Blokzincir ve dağıtık kayıt defteri teknolojileri – Dijital varlık saklama görevlilerinin güvenlik yönetimi

ISO/TS 23635:2022	Blokzincir ve dağıtık kayıt defteri teknolojileri – Yönetişim rehberi

Daha önce başlatılmış olan ISO/NP TR 23245 referans numaralı güvenlik riskleri ve zafiyetler konulu çalışma iptal edilmiştir.

Çizelge 2.24. ISO/TC 307 sorumluluğunda geliştirilmeye devam eden standartlar

Standart No	Standart başlığı
ISO/CD TR 3242	Blokzincir ve dağıtık kayıt defteri teknolojileri – Kullanım senaryoları
ISO/CD TR 6039	Blokzincir ve dağıtık kayıt defteri teknolojileri – Blokzincir sistemlerinin tasarımı için özne ve nesnelerin tanımlayıcıları
ISO/WD TR 6277	Blokzincir ve dağıtık kayıt defteri teknolojileri – Blokzincir ve dağıtık kayıt defteri kullanım senaryoları için veri akış modeli
ISO/AWI 7603	Özne ve nesnelerin tanımlanması için merkezi olmayan kimlik standardı
ISO/CD 22739	Blokzincir ve dağıtık kayıt defteri teknolojileri - Sözlük
ISO/AWI TS 23516	Blokzincir ve dağıtık kayıt defteri teknolojileri – Birlikte Çalışabilirlik Çerçevesi
ISO/WD TR 23642	Blokzincir ve dağıtık kayıt defteri teknolojileri – Akıllı sözleşme güvenliği iyi uygulamalarına ve sorunlarına genel bakış
ISO/CD TR 23644	Blokzincir ve dağıtık kayıt defteri teknolojileri – Dağıtık kayıt defteri teknolojisine dayalı kimlik yönetiminde güven çapalarına[3] genel bakış (TADIM)

ISO tarafından geliştirilen ve geliştirilmekte olan, konu ile ilgisi bulunan diğer standartlar ise aşağıda listelenmiştir:

- ISO/TC 68 – Finansal hizmetler: Ekim 2022 itibariyle 36 katılımcı, 48 gözlemci üye tarafından yürütülmekte olan çalışmalar kapsamında 72 adet yayınlanmış ISO standardı ile 28 adet üzerinde çalışılmakta olan standart bulunmaktadır. Bankacılık, menkul kıymetler ve diğer finansal hizmetlerle ilgili konuları kapsamaktadır.
- ISO/IEC JTC 1/SC 27 – Bilgi Teknolojileri Güvenlik Teknikleri standardı: Ekim 2022 itibariyle 52 katılımcı, 35 gözlemci üye tarafından yürütülmekte olan çalışmalar kapsamında, 224 adet yayınlanmış, 65 adet üzerinde çalışılmakta olan standart bulunmaktadır. Bilginin ve bilgi ve iletişim teknolojilerinin korunması için geliştirilmiş olan standartlardır.
- ISO/IEC JTC1 SC40 – Bilgi Teknolojileri Hizmet Yönetimi ve Bilgi Teknolojileri Yönetişimi standardı: Bilgi teknolojilerinin yönetişimi ve hizmet yönetimi konusunda denetim, dijital hukuk, risk yönetimi, dış kaynak kullanımı gibi konuları da içeren

[3] Güven çapası (trust anchor) hiyerarşik yapıya sahip kriptografik sistemlerde güvenilir sertifikalara sahip depolanan anahtarları gösteren, sertifika yollarını doğrulayan yapıdır.

standartları kapsamaktadır. Bu başlık altında Ekim 2022 itibariyle yayınlanmış olan 26, geliştirme aşamasında olan 11 standart bulunmaktadır.

- ISO TC309 – Kuruluşların yönetişimi standardı: İletişim ve görevlendirme, stratejik iş planı, rüşvetle mücadele yönetimi, uygunluk yönetimi gibi konuları içermekte olup Ekim 2022 itibariyle yayınlanmış olan dört standart bulunmaktadır. Yedi standart da henüz geliştirilme aşamasındadır.

2.2.2. Uluslararası Telekomünikasyon Birliği (ITU) faaliyetleri

Merkezi İsviçre-Cenevre'de olan, Birleşmiş Milletlere üye 193 ülke ve 700'den fazla Bilgi ve İletişim Teknolojisi (Information and Communication Technology - ICT) kuruluşu, akademik ve araştırma enstitüsünün üyesi bulunduğu Uluslararası Telekomünikasyon Birliği tarafından da blokzincir uygulamaları ve standardizasyonu üzerine çalışmalar yürütülmektedir.

ITU Telekomünikasyon Standardizasyon Sektörü (ITU-T), ITU-T Tavsiyeleri olarak bilinen uluslararası standartları geliştirmek için tüm dünyadan uzmanları bir araya getirerek çalışma grupları oluşturmakta, blokzincir ile ilgili olanlar da dâhil olmak üzere standardizasyon faaliyetlerini Avrupa Komisyonu tarafından yürütülen Bilgi ve İletişim Teknolojileri Standardizasyonu İlerleme Planına düzenli olarak raporlamaktadır.

Standardizasyondan önce, seçilen alanlardaki spesifikasyonların hızlı biçimde geliştirilmesi için ITU-T Odak Grubu, ITU-T Tavsiyeleri olarak adlandırılan uluslararası standartların geliştirilmesi için ise ITU-T Çalışma Grubu görev yapmaktadır. Ayrıca, dağıtık kayıt defteri uygulamaları konusunda çalışmak üzere 2017 yılı Mayıs ayında kurulmuş olan Dağıtık Kayıt Defteri Teknolojileri Odak Grubu (FG-DLT) ilk toplantısını 17-19 Ekim 2017 tarihinde yapmıştır. Blokzincir ve dağıtık kayıt defteri teknolojisi konusunda çalışan Çalışma Grubu 17 (Güvenlik), Çalışma Grubu 13 (Gelecekteki Ağlar), Çalışma Grubu 16 (Multimedya), Çalışma Grubu 20 (IoT, Akıllı kentler ve topluluklar-SCC, Nesnelerin Blokzinciri) gibi birçok çalışma grubu bulunmaktadır. Dağıtık Kayıt Defteri Teknolojileri Odak Grubu çalışmalarını 1 Ağustos 2019 tarihinde tamamlayarak aşağıda verilmiş olan Çizelge 2.25'teki çalışmaları yayınlamıştır (International Telecommunication Union, 2019).

Çizelge 2.25. ITU-T Dağıtık Kayıt Defteri Teknolojileri Odak Grubu yayınları

Yayın tipi	Numarası	Başlığı
Teknik Özellikler	FG DLT D1.1	Dağıtık Kayıt Defteri Teknolojileri terim ve tarifleri
Teknik Rapor	FG DLT D1.2	Dağıtık Kayıt Defteri Teknolojilerine genel bakış, kavramlar ve ekosistem
Teknik Rapor	FG DLT D1.3	Dağıtık Kayıt Defteri Teknolojileri standardizasyon ortamı
Teknik Rapor	FG DLT D2.1	Dağıtık Kayıt Defteri Teknolojileri kullanım senaryoları
Teknik Özellikler	FG DLT D3.1	Dağıtık Kayıt Defteri Teknolojileri referans mimarisi
Teknik Özellikler	FG DLT D3.3	Dağıtık Kayıt Defteri Teknolojileri platformları değerlendirme kriterleri
Teknik Rapor	FG DLT D4.1	Dağıtık Kayıt Defteri Teknolojileri düzenleyici çerçeve
Teknik Rapor	FG DLT D5.1	Dağıtık Kayıt Defteri Teknolojilerine genel bakış

2.2.3. Diğer standardizasyon faaliyetleri

Elektrik ve Elektronik Mühendisleri Enstitüsü (IEEE) Faaliyetleri

IEEE bünyesinde dünya çapında tanınan bir standart belirleme kuruluşu olan IEEE Standartları Derneği (IEEE SA), birden fazla endüstri sektöründeki çeşitli etkinlikler aracılığıyla aktif olarak blokzincir standardizasyon çabalarını sürdürmektedir. Hâlihazırda IEEE SA tarafından yürütülmekte olan çok sayıda standardizasyon çalışması bulunmakta olup bunlardan yayınlanmış olanların tamamı ile geliştirilme aşamasında olanların bir kısmı Çizelge 2.26'da verilmiştir (IEEE, 2022)

Çizelge 2.26. IEEE tarafından yürütülen standardizasyon çalışmaları (Geliştirme aşamasında olanların tamamı alınmamıştır)

Referans	Başlık	Durum
2140.1-2020	Kripto para Borsaları İçin Genel Gereksinimler IEEE Standardı	Yayınlandı
2140.2-2021	Kripto para Borsalarındaki Kripto Varlıklar İçin Güvenlik Yönetimi IEEE Standardı	Yayınlandı
2140.5-2020	Kripto Para Birimi Saklama (custodian) Çerçevesi IEEE Standardı	Yayınlandı
2142.1-2021	Blokzincir Teknolojisi Kullanılarak e-Fatura için IEEE Uygulama Tavsiyesi	Yayınlandı
2143.1-2020	Kripto para Ödemeleri Süreci İçin Genel IEEE Standardı	Yayınlandı
2144.1-2020	Blok Zinciri Tabanlı Nesnelerin İnterneti (IoT) Veri Yönetimi Çerçevesi için IEEE Standardı	Yayınlandı
2146.1-2022	Blockchain Teknolojisi aracılığıyla Kuruma Dayalı Risk Karşılıklı Yardım Modeli Standardı	Taslağı onaylandı
2418.2-2020	Blokzincir Sistemleri İçin Veri Formatı IEEE Standardı	Yayınlandı
2418.7-2021	Tedarik Zinciri Finansmanında Blockchain Kullanımı IEEE Standardı	Yayınlandı
2418.10-2022	Blockchain tabanlı Dijital Varlık Yönetimi IEEE Standardı	Yayınlandı
3801-2022	Blockchain Tabanlı Elektronik Sözleşmeler IEEE Standardı	Yayınlandı
P2140.3	Kripto para Borsalarında Kullanıcı Kimliği ve Kara Paranın Önlenmesi Standardı	Geliştirme aşamasında
P2140.4	Dağıtık Kayıt Defteri Kullanan Dağıtık/Merkeziyetsiz Borsa Çerçevesi Standardı	

P2141.1	Merkezi Kuruluşlar için Yolsuzlukla Mücadele Uygulamalarında Blokzincir Kullanımı Standardı	
P2143.2	Kripto para Ödemeleri Performans Metrikleri Standardı	
P2143.3	Kripto para Ödemeleri Risk Kontrol Gereksinimleri Standardı	
P2418.8	Devletlerde Blokzincir Uygulamaları İçin Standartlar	
P2418.10	Blokzincire Dayalı Dijital Varlık Yönetimi İçin Standartlar	

Avrupa Standardizasyon Komitesi (CEN) ve Avrupa Elektroteknik Standardizasyon Komitesi (CENELEC) Faaliyetleri

2017 yılında CEN ve CENELEC tarafından Avrupa için blokzincir ve dağıtık kayıt defteri teknolojileri standardizasyonundaki boşlukların belirlenmesi ve bu boşlukların ISO/TC 307'nin devam eden çalışma öğeleri ile eşleştirilmesi, uluslararası standardizasyon çalışmalarına katılarak bu çalışmaların desteklenmesi için ortak bir Blokzincir ve Dağıtık Kayıt Defteri Teknolojileri Odak Grubu kurulmuştur (ITU-T, 2019). Bu grup tarafından standart geliştirme faaliyeti yürütülmemekle birlikte ISO/TC 307 ve ITU-T ile temas halinde uluslararası standardizasyon çalışmalarına katılmaktadırlar.

Odak grubu, özellikle birlikte çalışabilirlik, sürdürülebilir kalkınma, güvenlik, gizlilik, kimlik, akıllı sözleşmeler, referans mimarileri ve kullanım senaryolarının belirlenmesi gibi konular üzerinde çalışmaktadır.

2.2.4. Blokzincir ve dağıtık kayıt defteri düzenlemeleri

Birçok faydasının yanında, blokzincir ve dağıtık kayıt defteri teknolojilerinin özellikle finans alanında istikrarı ve kritik hizmetlerin sunumunu olumsuz etkileme potansiyeli bulunmaktadır. Düzenleyici ve denetleyici kurumları devreden çıkarma potansiyeli özellikle finansal teknolojilere ilişkin mali ve operasyonel riskleri ortaya çıkarmaktadır. Bu nedenle, tüm dünya devletleri tarafından bu yeni teknolojilerin mevcut düzenlemeler tarafından kapsanıp kapsanmadığı, mevcut düzenlemelerde revizyon gerekip gerekmediği ve inovasyonu engellemeden risklere karşı önlemlerin nasıl alınabileceği konularında yoğun çalışmalar yürütülmektedir.

Özellikle finansal uygulamalar konusundaki düzenlemelerde genel olarak iki temel yaklaşım bulunmaktadır. Bunlar bağlayıcı olan hukuk (hard law) ve bağlayıcı olmayan hukuk (soft law) biçimindedir. Devletler ve düzenleyici kurumlar bu iki yaklaşımı genellikle bir arada

kullanmaktadırlar. Özellikle Bitcoin ve belirli bir merkezden yönetilmeyen, coğrafi bir merkezi ya da bağlılığı olmayan, düzenlenmesi, yasaklanması ve kontrol edilmesi güç olan finansal uygulamalar için bağlayıcı olmayan hukuk öne çıkmaktadır. Bağlayıcı olmayan hukuk bir bakıma piyasanın kendi kendini düzenlemesine ve dengelemesine müsaade edilmesi olarak da değerlendirilmektedir. Blokzincir teknolojisine dayalı finansal uygulamaların ilk zamanlarında çoğu devlet bekle ve gör yaklaşımını benimseyerek daha çok yatırımcıları ve vatandaşları uyarmakla yetinmiştir. Ancak özellikle 2017 yılından sonra kripto paraların ve ICO'ların sayısının çok artması, spekülasyonların çoğalması, bu teknolojinin vergi kaçırma, dolandırıcılık, yolsuzluk, kara para aklama ve terör ya da illegal faaliyetlerin finansmanında kullanılmaları gibi nedenler düzenleyici kurumları bağlayıcı düzenlemeler getirmeye yönlendirmiştir.

Mevcuttaki düzenlemeler değerlendirildiğinde, genellikle finans konusunda yapılan çalışmaların yoğunlukta olduğu görülmektedir. Finans konusundaki düzenlemelerin temelinde ise öncelikle kripto paraların tanımlanması yatmaktadır. Kripto paraların fiyat para, emtia ya da yatırım aracı olarak değerlendirilmesine göre farklı düzenlemeler geliştirilmekte olup genel bir uygulama birliği bulunmamaktadır. Bu alandaki düzenlemeler genel olarak finansal raporlama, müşterini tanı (KYC), kara paranın aklanmasının ve terörün finansmanının önlenmesi ve vergilendirme konularında yoğunlaşmaktadır. Ayrıca, tüketicinin ve yatırımcının korunmasına yönelik olarak da çalışılmakta olup birçok ülkenin ilgili kuruluşları tarafından bilgilendirici ve yönlendirici kılavuzlar yayınlanmaktadır. Teknolojinin gelişimini hızlandırıcı, iyi uygulama olarak değerlendirilebilecek olan ve aşağıda örnekleri verilmiş olan bazı devletlerce de uygulanan yaklaşım ise düzenleyici test alanlarıdır (regulatory sandbox). Düzenleyici test alanları kamu ve özel sektörün bir arada yönettiği, yeni iş modellerinin korunaklı bir ortamda test edilebildiği, düzenleyici ve denetleyici kurumlar ile özel teşebbüsün birlikte öğrendiği ve uygulama yaptıkları güvenli alanlardır. Bu test alanlarında tüm ülkeyi kapsayan yasal düzenlemeler yerine her firma ya da iş modeline göre hazırlanmış düzenlemeler söz konusudur. Tüketicinin korunması için uygulamalar belirli bir zaman için, belirli sayıdaki tüketici ya da müşteri ile deneyimlenir. Test ortamında bireysel rehberlik verilerek proje özelinde yasal düzenlemelerden feragat edilebilir ve yaptırımlardan kaçınılır. Bu modele ilişkin ilk örnek Birleşik Krallık'tır. Singapur, Abu Dabi, Avustralya, Kanada Danimarka, Hong Kong, İsviçre, Malezya ve Güney Afrika da İngiltere'yi takiben test alanları oluşturan diğer ülkelerdendir.

Davradakis ve Santos (2019) politika hedeflerinin çoğunlukla tüketicinin korunması, piyasa bütünlüğü ve finansal sisteme katılımın sağlanması kadar rekabetin ve inovasyonun teşvik edilmesini de içerdiğini öne sürmektedir. Düzenlemelerle ilgili değişikliklerin odaklandığı konular kitlesel fonlama (crowdfunding), fintek kredisi, sanal para birimleri, ödemeler, siber güvenlik ve büyük veri, bulut bilişim gibi yeni teknolojilerdir. Yeniliklere ve denemelere rehberlik etmek için ilgili kurumların kullandığı en yaygın model yeni ürün veya hizmetlerin kontrollü bir ortamda test edilebildiği düzenleyici sanal alanlardır. Bu yaklaşım Avustralya, Kanada, Hong Kong, Güney Kore, Hollanda, Singapur ve İngiltere tarafından kullanılmaktadır. Bir başka modelde ise Japonya, Güney Kore, Brezilya ve Fransa'da örnekleri görülen, firmaların düzenlemelere uyum sağlamalarına destek olan Fintek Destek Merkezleri yer almaktadır. Son olarak, kullanım alanlarını geliştirmek ve büyümeyi hızlandırmak için geliştiriciler, firmalar ve kamu kurumları arasında işbirliği ve ortaklık düzenlemeleri yapılmaktadır. Sanal paralar dışında blokzincir teknolojisinin kullanımı ise bu teknolojinin yasal olarak regüle edilmiş kurumlarca, kapalı bir sistemde kullanılmasından dolayı yasal düzenlemeler konusunda daha az endişe doğurmaktadır.

Kripto paralarla ilgili yasadışı faaliyetlerden en önemlileri yasadışı ürün ya da hizmet satışı, kara para aklama, sermaye kontrollerinden kaçınma, fidye saldırılarında ödeme aracı olarak kullanım ve hırsızlıktır. Kripto paraların bu yapısal risklerinin yanı sıra son yıllardaki fon toplama aracı olarak kullanılan tokenların sayısındaki büyük artış ve sabit kripto para birimlerinin (stablecoin) ve merkez bankası dijital paralarının ortaya çıkması gibi gelişmeler kripto para terimi yerine kripto varlık teriminin kullanılarak yasal düzenlemelerin tüm bu varlıkları kapsayacak şekilde genişletilmesi ihtiyacını doğurmuştur. Avrupa Birliğince bu ihtiyaca binaen 30 Mayıs 2018 tarihinde Beşinci Kara Paranın Aklanmasının Önlenmesi Direktifi (AMLD5) kabul edilmiştir. Yapılan düzenlemeler ile müşterilerin daha iyi tanımlanması ve azami özenle daha az anonimlik ve daha fazla izlenebilirliğin sağlanması hedeflenmiş, saklama cüzdanı sağlayıcıları ile sanal para alışveriş platformları yasa kapsamına alınmıştır.

Avrupa Adalet Divanının 22 Ekim 2015 tarihinde aldığı karar doğrultusunda, tüm AB üye ülkelerinde Bitcoin alış ve satış işlemleri KDV'den muaftır. Avrupa menkul kıymetler, bankacılık, sigorta ve emeklilik denetleme birimlerinin 12 Şubat 2018 tarihinde yayınladıkları ortak bildiri ile tüketiciler sanal paraların yüksek risk taşıdıkları, yasal düzenlemelerinin bulunmadığı ve yatırım, tasarruf veya emeklilik planlama ürünü olarak

uygun olmadıkları konusunda uyarılmıştır (The Law Library of Congress, Global Legal Research Center, 2018: 29).

Houben ve Snyers (2020), kripto dünyasındaki hızlı gelişmelere karşı AB'nin düzenleme faaliyetlerinde kripto para tanımının kapsamının token gibi kavramları da içerecek biçimde genişletilmesini, yükümlü kuruluşların listesinin genişletilerek kripto para alışveriş hizmeti sağlayan, kripto ticaret platformu işleten, cüzdan hizmeti sunan işletmeler gibi düzenlemelerin dışında kalmış işletmelerin kapsama alınmasını, özellikle kara paranın aklanmasının izlenmesi için Bilgi Teknolojileri konusunda uzman çalışanlar istihdam edilerek yeni teknolojilerden kaynaklanan risklerin analiz edilmesini, mevcut yasal düzenlemelere uyumun AB ve üye ülke kuruluşları düzeyinde denetlenmesini önermektedir. Düzenlemelerde dikkate alınması gereken diğer iki konu tüketici ve yatırımcıların korunması ve siber güvenliktir.

Dünyada kripto varlıklara ilişkin yasal düzenlemelere bakıldığında hemen hemen tamamının finansal alanlara ilişkin olduğu görülmektedir. Detaylarına tezde yer verilmemiş olan bu yasal düzenlemelerde öne çıkan konular aşağıdaki biçimdedir:

- Tüketici ve yatırımcının gerekli hallerde korunması ile inovasyonun engellenmesi arasında dengenin kurulması hedeflenmektedir,
- Avrupa Birliği üyesi ülkelerde genel olarak ortak mevzuata dayalı bir yaklaşım gösterilmektedir,
- Yasal düzenlemelerin yapılabilmesi için öncelikle kripto varlıkların tanımlanması, statülerinin belirlenmesi ve bu varlıkların sınıflandırılması (menkul kıymet, yatırım aracı, kripto para vb.) gerekmekte olup birçok ülke öncelikle bu sınıflandırma ve tanımlamaları yapmaktadır,
- Kripto paraların sınır tanımayan doğası ve kontrol edilmesinin güçlüğü birçok ülkenin özellikle 2017 yılı ve öncesinde süreci izlemekle ve vatandaşları kripto paraların risklerine karşı uyarmakla yetinmesine sebep olmuştur,
- Düzenlemelerde öne çıkan konuların başında kara paranın aklanmasının ve terörün finansmanının önlenmesi ile müşterini tanı yükümlülüğü gelmektedir,
- Düzenlemelerde öne çıkan diğer konular ise kripto para ticareti yapan, kripto varlık ticareti için platform sağlayan, cüzdan hizmeti veren işletmeler için lisans, kayıt, bildirim ve raporlama yükümlülüğünün getirilmesi, madencilik ve kripto para ticaretinden elde

edilen kazançların vergilendirilmesi, kripto varlık türev işlemlerinin düzenlenmesi, büyük miktarlı transferler, yurtdışına yapılan transferler, tespit edilemeyen taraflar arasındaki yüksek hacimli işlemler gibi şüpheli hareketlerin bildirimi biçimindedir,

- Bitcoin, Litecoin ve Ethereum gibi merkezi olarak yönetilmeyen kripto paraların düzenlenmesinde güçlük yaşanmakta, bu kripto paralar için lisans gereklilikleri uygulanamamaktadır,
- Kripto paraların vergilendirilmesinde kullanılacak kazanç miktarı ile ödemelerde kullanılacak para birimi arasında kur dönüşümü hesaplamaları güçlük yaşanan bir diğer konudur.

Yapılan literatür araştırması sonucunda Avrupa Birliği ve 65 ülkede yapılmış olan yasal düzenlemeler incelenmiş olup bu düzenlemelerin finans alanında yoğunlaştığı, birçok ülkenin yatırımcıları ve vatandaşları özellikle kripto paraların risklerine karşı resmi uyarılar yayınladıkları tespit edilmiş olup bu yasal düzenlemelerin sınıflandırılmasına ilişkin bilgiler Çizelge 2.27'de, ülkelere göre bu düzenlemelerin adetleri de Çizelge 2.28'de verilmiştir.

Çizelge 2.27. Avrupa Birliği ve dünya ülkeleri tarafından yayınlanan düzenleme sayıları

Düzenleme tipi/konusu	**Adet**
Resmi uyarı	51
Yasal düzenleme (finans)	37
Kara Paranın Aklanmasının ve Terörün Finansmanının Önlenmesi	22
Rehber	20
Yasal düzenleme (kripto para)	20
Düzenleyici sanal test alanı	12
FinTek Destek Merkezi	6
Müşterini Tanı (KYC) yükümlülüğü	5
GDPR	2
Yasal düzenleme (blokzincir)	1
Rapor	1
Toplam	**177**

Çizelge 2.28. Ülkelere göre yasal düzenleme sayıları

Ülke	**Adet**	**Ülke**	**Adet**	**Ülke**	**Adet**	**Ülke**	**Adet**
Avrupa Birliği	12	Güney Afrika	3	Slovakya	2	Namibya	1
Avusturya	9	Kanada	3	İrlanda	2	Letonya	1
İsviçre	8	Rusya	3	İsrail	2	Nepal	1
İngiltere	7	Filipinler	3	Katar	2	Tacikistan	1
Avustralya	7	Malezya	3	Zimbabve	1	Gana	1

Ülke	Adet	Ülke	Adet	Ülke	Adet	Ülke	Adet
Japonya	7	ABD	3	Ürdün	1	Uganda	1
Singapur	6	Estonya	3	Tayland	1	Özbekistan	1
Fransa	6	Arjantin	3	Macaristan	1	Umman	1
İtalya	5	Portekiz	2	Endonezya	1	Pakistan	1
BAE	4	Norveç	2	Hırvatistan	1	Lübnan	1
Hollanda	4	Finlandiya	2	Suudi Arabistan	1	Çekya	1
Çin	4	İsveç	2	Bulgaristan	1	İspanya	1
Yeni Zelanda	4	Polonya	2	Ukrayna	1	İran	1
Almanya	4	Lüksemburg	2	Mısır	1	Belçika	1
Brezilya	4	Romanya	2	Yunanistan	1	Kenya	1
Malta	4	Danimarka	2	Mozambik	1		
Güney Kore	4	Hindistan	2	Zambiya	1		
						Toplam	**177**

Houben ve Snyers (2020) kripto varlıkların küresel bir fenomen olduğunu belirterek sınır tanımayan yapısı, dünyanın her yerinden kolaylıkla erişilebilmesi, transfer edilebilmesi ve ticaretinin yapılabilmesi nedeniyle yasal düzenlemelerin ülkeler tarafından münferit yapılmasındansa mümkünse uluslararası standartları da belirlenerek, Avrupa düzeyinde, tüm ülkeleri içine alacak biçime yapılması gerektiğini belirtmektedir. Aynen kara paranın aklanmasının ve terörün finansmanının önlenmesinde olduğu gibi, kripto varlıklarla ilgili illegal faaliyetler de yasal düzenlemenin olmadığı ya da nispeten daha zayıf olduğu ülkelere kayma eğilimindedir. Yasal düzenlemelerin ülke ya da bölge düzeyinde yapılması nihai risklerin ortadan kaldırılmasında yeterli olmayacaktır. Bu nedenle, olabildiğince küresel çapta geçerli standartlar ve kuralların getirilmesi gerekmektedir.

2.3. Uluslararası Kuruluşlar ve Devletlerce Yürütülen Çalışmalar

Her yeni teknolojide olduğu gibi blokzincir konusunda da gerek kamu gerekse özel sektör kuruluşları arasında hem kıyasıya bir yarış yaşanmakta hem de işbirliği faaliyetleri yürütülmektedir. Temelinde finans sektörünün lokomotif görevi gördüğü blokzincir teknolojisi devletler, akademik dünya, özel sektör temsilcileri ve uluslararası kuruluşlarca yakından takip edilmektedir. Başlangıçta araştırma faaliyetlerinin ağırlıkta olduğu çalışmalar zamanla proje ve prototip geliştirme aşamasına geçmiş, son zamanlarda ise gerçek kullanım örnekleri ortaya çıkmaya başlamıştır.

Dünya Ekonomik Forumu'na (2018) göre blokzincirin 2013'de 1 milyar $ olan pazar değeri 2025 yılında 176 milyar $'ı, 2030 yılında ise 3,1 trilyon $'ı aşacaktır. Dağıtık kayıt defterleri ve blokzincirin dönüştürücü gücünü fark eden Dünya Bankası 2017 yılında pilot projeler yürütmek ve sosyal ve yönetsel çıktıları geliştirmek için bir blokzincir laboratuvarı kurmuştur. Laboratuvarın hedefi öğrenme, denemeler yapma ve iş ve dış paydaşlarla blokzincir uygulamaları konusunda işbirliğini geliştirmektir.

23 Ağustos 2018 tarihli basın bildirisi ile Dünya Bankası dağıtık kayıt defteri teknolojisi kullanılarak yaratılan, tahsis edilen, transfer edilen ve yönetilen dünyanın ilk tahvili olan bond-i (Blockchain Operated New Debt Instrument - blokzincir ile işletilen yeni borçlanma aracı) adı verilen tahvili piyasaya sürdüğünü duyurmuştur. Sürdürülebilir kalkınmayı desteklemek için yıllık 50 – 60 milyar dolarlık tahvil çıkaran Dünya Bankası'nın çıkardığı bu tahvil iki yıl süreli olup 73 milyon dolar değerindedir. Dünya Bankası Washington Ofisi ve Commonwealth Bank of Australia (CBA) tarafından işletilen bond-i Microsoft Azure bulut platformunu kullanmaktadır.

Avrupa Birliği ve Birleşmiş Milletler başta olmak birçok uluslararası kuruluş, birlik ve devletler tarafından yürütülen faaliyetlerin detayları aşağıda verilmektedir.

2.3.1. Avrupa Birliği Faaliyetleri

Avrupa Birliği (AB) bünyesinde blokzincir teknolojisi konusunda araştırma, raporlama, mevzuat ve uygulamaya dönük yoğun çalışmalar yürütülmektedir. Bu çalışmaları etkin bir biçimde yürütmek ve münferit çalışmalar yerine ortak bir merkez üzerinden çalışmaları konsolide etmek üzere AB tarafından gerçekleştirilmiş olan en önemli iki faaliyet 2017 yılında ihalesi düzenlenen Avrupa Blokzincir Gözlemevi ve Forumu'nun ve 2018 yılında 2020 yılı itibariyle AB üyesi olmayan Birleşik Krallık, Norveç ve Lihtenştayn da dahil 30 üyesi bulunan Avrupa Blokzincir Hizmetleri Altyapısının (EBSI) kurulmasıdır.

Probst, Frideres, Cambier ve Martinez-Diaz (2016), Avrupa Komisyonu İş İnovasyon Gözlem Merkezi adına hazırladıkları resmi olmayan raporda, blokzincir uygulamaları ve hizmetleri konusunda faaliyet gösteren yedi firmanın dâhil olduğu, blokzincir konusuna yönelik eğilimler, sektörü yönlendiren unsurlar ve karşılaşılan zorlukları analiz ederek bir vaka çalışması gerçekleştirilmiştir. Bu analizlere dayanarak Avrupa Komisyonu'na

sunulmak üzere hazırlanan raporda işbirliğinin kolaylaştırılması, standartların geliştirilmesine destek verilmesi, uygun düzenleyici çerçeve geliştirilerek endüstrinin genişlemesi için farkındalığın artırılması ve zihniyet değişimi olmak üzere dört ana başlıkta politika tavsiyelerine yer verilmiştir.

AB bünyesinde gerçekleştirilen ilk çalışmalardan biri Avrupa Parlamentosu'nun 26 Mayıs 2016 tarihli ve P8_TA(2016)0228 sayılı kararıdır. Avrupa Konseyi ve Komisyona sunulmak üzere alınan sanal para birimleri konulu bu karar sanal paralar ve dağıtık kayıt defteri teknolojilerinin riskleri ve sunduğu fırsatları, para politikalarına olası etkilerini, ödemelerde kullanılmasını ve bu teknolojinin testi için devletlerin teşvik edilmesi konularını içermektedir.

Avrupa Komisyonu 2016 yılında 3 yıl süreli ve 5 milyon € bütçeli Merkezi Olmayan Vatandaş Veri Ekosistemi (Decentralised Citizen Owned Data Ecosystem - DECODE) adlı bir proje başlatmıştır. DECODE projesi insanların kendi çevrimiçi verilerini yönetebilmelerini sağlayarak bu veriler üzerindeki kontrollerini artıracak blokzincire dayalı araçları test etmek ve geliştirmek amacını taşımaktadır. Projeye İspanya, Hollanda, İtalya, İsveç, Fransa ve İngiltere'den 14 kuruluş destek vermektedir. DECODE projesi 80 milyar € bütçesi ile en büyük AB Araştırma ve İnovasyon Programı olan Horizon 2020'nin bir parçasıdır (DECODE, tarih yok).

2017 yılı Haziran ayında, blokzincir teknolojisinin finans dışındaki sektörlerde mevcut, üzerinde çalışılan ve potansiyel uygulamaları konusunda araştırmalar yürütmek üzere Avrupa Komisyonu Ortak Araştırma Merkezi ve İç Pazar, Sanayi, Girişimcilik ve KOBİ Genel Müdürlüğü tarafından Blockchain4EU adlı proje başlatılmış, bu kapsamda ayrıca AB Politika Laboratuvarı kurulmuştur. Yaratıcılığı ve katılımı teşvik etmek, AB politikalarının geliştirilmesine yardımcı olacak etkileşimler, süreçler ve araçlar geliştirmek için öngörü, modelleme, davranışsal içgörüler ve politika tasarımı olmak üzere dört tamamlayıcı boyut etrafında çalışmalar yürüten bu laboratuvar test etme, deney yapma ve birlikte tasarlama konularında paydaşları bir araya getirmekte, işbirliğini kolaylaştırmak için hem fiziksel hem de kavramsal bir alan olarak hizmet vermektedir.

21 Temmuz 2017'de Avrupa Komisyonu (2017) tarafından 500 bin € bütçeli "Avrupa Blokzincir Gözlemevi ve Forumu: Blokzincir ve Dağıtık Kayıt Defteri Teknolojileri Üzerine

Bir Avrupa Uzmanlık Merkezi Kurulması ve İşletilmesi" konulu ihale şartnamesi yayınlanmıştır. Bu ihale kapsamında iki yıl sürmesi planlanan projenin temel amacı blokzincir ve dağıtık kayıt defteri teknolojisi konusunda kapasite oluşturulması, bilgi toplanması ve bilginin yayılması için bir merkez kurulması olarak belirlenmiştir.

2018 yılı Nisan ayında birçok AB ülkesi tarafından teknik ve yasal uzmanlığın paylaşımının sağlanarak işbirliğinin geliştirilmesi için Avrupa Blokzincir Ortaklığının kurulmasına dair bir deklarasyon imzalanmıştır (Perchet, Loget ve Daniel, 2020). Bu deklarasyon ve kurulan ortaklığın sonucunda, 1 Şubat 2018 tarihli basın bildirisi ile Avrupa Komisyonu (2018) AB Blokzincir Gözlemevi ve Forumu'nun Avrupa Parlamentosu'nun da desteğiyle devreye alındığını duyurmuştur. Aynı basın bildirisinde Avrupa Komisyonu'nun blokzincir projelerini FP7 ve Horizon 2020 araştırma programları kapsamında 2013 yılından bu yana desteklediği belirtilerek 2020 yılına kadar blokzincir teknolojilerinden yararlanan projelere 340 milyon €'ya kadar finans desteği sağlanacağı bildirilmiştir.

AB bünyesinde blokzincir konusunda kapasite geliştirmek için kurulmuş olan bu Gözlemevi ve Forum kurulduktan sonraki iki yıl içinde teknolojinin gelişiminin hızlandırılması ve ihtiyaç duyulan bilgi desteğinin sağlanması için sosyal medya ve web sayfası üzerinden yoğun biçimde bilgi paylaşımı yaparak 800'den fazla tweet ile 9 500 takipçiye, 2 600 bülten abonesine, 2 200 web sayfası üyesine, youtube platformunda 8 500'ün üzerinde izlenme rakamına erişmiş, web sitesini iki yıl içinde 91 bin kişi ziyaret ederek 310 bin sayfa görüntülenmiştir (EU Blockchain Observatory and Forum, 2020). AB Blokzincir Gözlemevi ve Forumu tarafından Mayıs 2018 – Ekim 2022 tarihleri arasında 35 tematik rapor hazırlanmış, her birinin sonuç raporu yayınlanmış olan 36 çalıştay düzenlenmiştir.

2016 yılı Aralık ayında Avrupa Merkez Bankası ile Japonya Merkez Bankası tarafından dağıtık kayıt defteri teknolojilerinin finansal konularda muhtemel kullanım alanlarını araştırmak üzere Stella adlı ortak bir proje başlatmıştır (The Law Library of Congress, Global Legal Research Center, 2018: 30). Projenin ilk evresi Dağıtık Kayıt Defteri Teknoloji kullanılarak büyük ölçekli ödemelerin işlenmesine odaklanmış ve 2017 yılı Eylül ayında yayınlanan rapor ile tamamlanmıştır. İkinci evre ise Dağıtık Kayıt Defteri ortamında ödeme karşılığı menkul kıymet teslimine odaklanmış ve 2018 yılı Mart ayında yayınlanan raporla tamamlanmıştır. Senkronize sınır ötesi ödemelere odaklanan üçüncü fazın tamamlanmasına ilişkin rapor ise Haziran 2019'da yayınlanmıştır. Dördüncü fazın teması ise gizlilik ile

denetlenebilirliğin dengelenmesidir. Avrupa Merkez Bankası dağıtık kayıt defteri teknolojilerini de içeren fintek çözümlerini çok dikkatli biçimde izlemektedir.

Dünya Bankalararası Finansal Telekomünikasyon Derneği (The Society for Worldwide Interbank Financial Telecommunication - SWIFT) tarafından ticaret finansmanında blokzincir kullanımı için yedi büyük Avrupa bankasının (KBC, Deutsche Bank, HSBC, Natixis, Rabobank, Société Générale ve UniCredit) oluşturduğu bir girişim duyurulmuştur. Dijital Ticaret Zinciri adı verilen bu girişim ile hem yerel hem de uluslararası ticarette alışveriş işlemleri için açık bir hesabın blokzincire dayalı bir platform aracılığıyla yönetilerek özellikle orta ölçekli işletmeler için Avrupa'da işlem maliyetlerinin azaltılması hedeflenmektedir (Niforos, 2017: 35).

Avrupa'da blokzincir ve enerji alanında olgunluk ve hazır olma bakımından en gelişmiş girişim olan Enerchain adlı proje ile 40'tan fazla işletme arasında gerçek zamanı olarak enerji ve doğalgaz ticareti gerçekleştirilmektedir (Merz, 2018: 5, 6)

Avrupa'nın en büyük 7 bankası Linux vakfı tarafından geliştirilmiş açık kaynak kodlu blokzincir projesi olan Hyperledger Fabric temelli IBM blokzincire dayanan yeni bir ticaret finansmanı platformunu kurmak ve işletmek için bir konsorsiyum kurmuştur. Konsorsiyumun amacı Avrupa'da küçük ve orta ölçekli işletmelerin yurtiçi ve uluslararası hizmet ticareti ödemelerini geliştirmektir (Groenfeldt, 2017).

2.3.2. Birleşmiş Milletler Faaliyetleri

Birleşmiş Milletler bünyesindeki birçok kuruluş blokzincire ilişkin araştırma, prototip geliştirme ve uygulama geliştirme faaliyetlerini yürütmektedir.

Birleşmiş Milletler Dünya Gıda Programı (WFP) tarafından Ürdün'de mülteci kampında yaşayan 106 bin Suriyeli mülteciye 2017 yılı Mayıs ayında başlatılmış olan "Building Blocks" adlı pilot proje kapsamında blokzincire dayalı bir sistemle gıda yardımı yapılmaktadır. Bu kamplarda hayatlarını sürdüren mültecilerin Birleşmiş Milletler Mülteciler Yüksek Komiserliği'nde kayıtlı biyometrik verileri ile entegre edilmiş olan blokzincir sistemi ile mülteciler sadece iris taraması ile marketlerden alışveriş yapabilmektedir. Bu proje ile finansal işlem ücretlerinden tasarruf etmenin yanında gizlilik

ve güvenlik sağlanmakta, yardımların amacına uygun biçimde kullanılması izlenebilmektedir (World Food Programme, 2020; Fridgen ve diğerleri, 2018).

Avrupa'nın en yoksul ülkelerinden biri olan Moldova çocuk ticaretini engellemek için Birleşmiş Milletler uzmanları ile birlikte blokzincire dayalı dijital bir çözüm üzerinde çalışmaktadır. Uluslararası gözlemcilere göre her yıl yüzlerce Moldovalı kadın ve genç kız Rusya, Türkiye ve Birleşik Arap Emirliklerine kaçırılmaktadır. Özellikle kırsal kesimde yaşayan çocuklar risk altında olup buralarda yaşayanların resmi olarak kimlik kayıtlarının bulunmaması onları kolay hedef haline getirmekte, sahte belgelerle sınır dışına çıkarılmalarını kolaylaştırmaktadır. Blokzincir ile, kağıt ortamında olmayan, parmak izi veya yüz tarama gibi biyometrik verilerle oluşturulmuş dijital kimlikler bu sahte belgelerle sınırı geçme olayını imkansız hale getirecektir. Bir önceki yıl çoğunluğu kadınlar ve kız çocukları olmak üzere yaklaşık 40 milyon insanın kaçırılarak zorla çalıştırıldığı ya da evlendirildikleri tahmin edilmektedir. Birleşmiş Milletler Proje Hizmetleri Ofisi (UNOPS) tarafından 2017 yılında bu suçla savaşmak için blokzincir teknolojisine dayalı bir pilot çalışma başlatmak üzere Dünya Kimlik Ağı adlı bir grup oluşturmuştur. Bu projeye somut ilgi gösteren ilk ülke Moldova olmuştur (Bacchi, 2017).

Birleşmiş Milletler kuruluşları, Microsoft ve Accenture gibi özel sektör şirketleri ve Rockefeller Vakfı arasında kurulmuş olan ID2020 girişimi blokzincir teknolojisi kullanılarak kimlik sağlanması, bunun için açık bir standart ve birlikte çalışabilir bir uygulama program arayüzü (API) geliştirilmesi ile hem dünya üzerindeki 1.1 milyar resmi kimliği olmayan insana hem de kamu sektörüne muazzam katkı sağlama potansiyeline sahip bir girişimdir (Berryhill ve diğerleri, 2018).

Birleşmiş Milletler Kalkınma Programı (UNDP), UNICEF ve Dünya Gıda Programı (WFP) ortaklığındaki BM İnovasyon Ağı, herhangi bir BM kuruluşunun blokzincir teknolojisini öğrenmesine ve denemesine olanak tanıyan kurumlar arası bir platform olan The Atrium'u başlatmıştır. Atrium, girişten ileri seviyeye öğrenme kaynaklarının düzenlendiği bir listeye ve bireylerin proje belgelerini ve kodunu paylaşabileceği bir BM blokzincir tabanlı projeler havuzuna sahiptir. BM kuruluşları bir projeye sıfırdan başlamak yerine, daha önce yapılmış olan işlerden faydalanabilmekte ve bunları ihtiyaçlarına göre özelleştirebilmektedir. Atrium'da özel bir Ethereum blokzincir çalıştırılmakta, böylelikle uygulamalar hızlı bir şekilde test edilebilmektedir (United Nations Innovation Network, 2020).

Birleşmiş Milletler İnovasyon Ağı tarafından Birleşmiş Milletler içerisindeki herkese açık olan bir Blokzincir Öğrenme Grubu ve beş hafta süren, katılımcıların kendi akıllı sözleşmelerini yazdıkları bir Blokzincire Giriş kursu başlatmıştır. Birleşmiş Milletler bünyesinde merkezi olmayan finans, Merkez Bankası Destekli Dijital Paralar (CBDC) ve fiziksel varlıkların blokzincirle sayısallaştırılması gibi konularda çalışmak ve üst yönetime tavsiyelerde bulunmak üzere bir Kripto Para Çalışma Grubu oluşturulmuştur. Birleşmiş Milletler tarafından yürütülen diğer bazı blokzincir projeleri ise aşağıda verilmiştir (United Nations Innovation Network, 2020):

- Afganistan Arazi Kayıt Yönetimi; Birleşmiş Milletler Bilgi ve İletişim Teknolojileri Ofisi (UN-OICT) tarafından yürütülen proje ile Afganistan'da arsa parsellerinin sahiplik bilgileri blokzincirle izlenmektedir.
- Cibuti ile Etiyopya Arasına Şeffaf Tedarik zinciri; Dünya Gıda Programı (WFP) tarafından yürütülen pilot proje ile iki ülke arasındaki ticari malların hareketleri izlenmekte, tedarik zincirinin şeffaflığı artırılarak bürokratik işlemlerin külfeti azaltılmaktadır. Proje ile, daha önce 15 – 20 gün alan nakliye sürecinin 3 – 5 güne düşürüleceği tahmin edilmektedir.
- Ürdün'deki Mülteci Kamplarına Nakit Transferi; WFP ve Birleşmiş Milletler Kadın Birimi (UN Women) tarafından yürütülen proje ile 100 000'den fazla Suriye'li mülteciye biyometrik kimlik doğrulama teknolojisi ve blokzincir teknolojisi kullanılarak gıda temini için nakit yardımı yapılmaktadır. Bu sayede hem havale ücretinden tasarruf edilmekte, hem de mültecilerin gizliliği ve güvenliği sağlanmaktadır.
- Ekvador'da Çikolata Üretiminin İzlenmesi; Birleşmiş Milletler Kalkınma Programı (UNDP) tarafından yürütülen pilot proje ile çikolata satın alındığında tüketicinin doğrudan çiftçiye geri gönderebileceği ya da gelecekteki ürün satın alımlarında indirim için kullanabileceği bir etki tokeni verilmekte, bir çiftçiye dört token gönderildiğinde yeni bir kakao ağacı dikilmektedir.
- UNICEF tarafından ilk defa 2019 yılı Ekim ayında yeni girişimleri destelemek için kripto paralarla kaynak toplanan bir fon kurulmuştur.
- Birleşmiş Milletler Bilgi ve İletişim Teknolojileri Ofisi bünyesinde, çalışanları teşvik etmek ve çalışanlar arasındaki işbirliği ve dayanışmayı geliştirmek için Unite Token adlı bir kripto varlık çıkarılmıştır. Yılın başında çalışanlara belirli bir miktar Unity Token verilmekte, yıl içerisinde çalışanlar birbirlerine destek olmak ya da teşekkür etmek için

bu tokenleri kullanmaktadır. Yılın sonundaki toplam tokenlar ise yöneticiler tarafından görülememekte, sadece eş çalışanlar birbirlerinin varlıklarını görebilmektedir.

- UNICEF Güney Afrika ve UNDP Güney Afrika tarafından yürütülen Zlto adlı dijital ödül sistemi ile gençler yerine getirdikleri mikro işler karşılığında dijital bir ödül kazanmakta, daha sonra topladıkları bu ödül karşılığında eğitim, resmi iş, küçük ölçekli girişim finansmanına erişim gibi teşvikler elde etmektedirler.

2.3.3. Devletler tarafından yürütülen faaliyetler

Kamu yönetimi bilimindeki e-devlet paradigmasının yerini artık dijital devlet kavramı almıştır. Eski model basitçe kamu yönetiminin dijitalleşmesini işaret ederken dijital devlet, dijital teknolojileri ve kamu ve vatandaşa ait bilgi varlıklarını kullanan yeni kamu hizmetlerinin ve hizmet sunum modellerinin yaratılması anlamına gelmektedir. Bu yeni paradigma kullanıcı merkezli, çevik ve yenilikçi kamu hizmetlerinin sağlanmasına odaklanmaktadır. Blokzincir teknolojisi de bu bağlamda politika oluşturma ve hizmet sunumu konularında devletlerin dikkate alması gereken en yenilikçi dijital teknolojilerden biridir (Allessie ve diğerleri, 2019).

Diğer tüm yenilik ve teknolojilerde olduğu gibi blokzincir teknolojisinde de araştırma çalışmaları ile geliştirme ve uygulama çabalarını kamu, özel sektör ya da akademik dünya olarak keskin sınırlarla ayırmak mümkün değildir. Berryhill ve diğerleri (2018) devletlerin blokzincir teknolojisinin kamu sektöründe kullanımı konusunda çalışmak üzere kamu özel işbirlikleri (PPP) ve farklı sektörler arasında (kamu sektörü, sivil toplum ve sanayii gibi) uygulamalar geliştirmek üzere birlikler oluşturduğunu öne sürmektedir. Bu tip anlaşmalar yönetimler arasında sürekli artmakta olup blokzincir sistemlerinin geliştirilmesi konusunda kamu kuruluşları ile özel sektör firmalarının bir araya getirilmesi için çaba gösterilmektedir. Bu çabalara örnek olarak Hyperledger gibi büyük konsorsiyumlar, İsviçre'deki Kripto Vadisi Birliği (Crypto Valley Association), ABD'deki Blokzincir Teminat Hızlandırıcı (Blockchain Trust Accelerator) veya Hindistan'daki Blokzincir ve Sanal Para Birimi Birliği verilebilir. Bunların tamamı, blokzincir teknolojisi ile ilgili tüm farklı aktörleri aynı hedefler doğrultusunda bir araya toplamayı amaçlamaktadır. Bu sektördeki kamu özel ortaklığına bir örnek de Birleşmiş Milletler kuruluşları, Microsoft ve Accenture gibi özel sektör şirketleri ve Rockefeller Vakfı gibi vakıflar arasında kurulmuş olan ID2020 girişimidir.

Hileman ve Rauchs (2017) kamu sektöründe blokzincir teknolojisi konusunda yürütülen çalışmalarda merkez bankalarının öne çıktığını belirtmektedir.
Blokzincir konusunda teknik uzmanlığın ve bilginin eksikliği yüzünden kamu ve özel sektör arasındaki bağ ve PPP'lerin gelişim hızı henüz istenen düzeyde değildir. Devlet içerisinde kodlama yetkinliğine sahip insan kaynağı oldukça kısıtlıdır. Smart Dubai Ofisi bu sorunun farkına vararak 14 000 memura veri okuryazarlığı kursu vermiştir. Kamu sektörü kodlama ile ilgili gereksinimlerini özel sektörden dış kaynak kullanımı ile tedarik edebilir ancak blokzincir teknolojisinin anlaşılması ve arzu edilen etkiyi göstermesi için kamı kurumlarının bünyesinde de bir insan kaynağının olması çok kritiktir. Blokzincir protokolleri ve uygulamalarının tasarımında uygun kararların verilmesi ve özel verilerin korunması devletlerin sorumluluğundadır (Berryhill ve diğerleri, 2018).

Dünya üzerindeki hemen her ülkede blokzincir teknolojisi ile ilgili yapılan çalışma örneklerine farklı haber sitelerinde rastlanmakla birlikte, bu çalışmada güvenilir kaynaklardan doğrulanabilen örneklere yer verilmiştir. Ayrıca, dünya üzerindeki çalışmalar araştırılırken Birleşmiş Milletler (2022) tarafından her iki yılda bir yayınlanan E-Devlet Araştırması Raporunda yer alan E-Devlet Gelişmişlik İndeksi (EGDI) esas alınarak ülkeler buradaki derecelerine göre sıralanmıştır. Türkiye, 2022 yılı araştırma raporunda bu listede 193 ülke içerisinde 48 inci sırada yer almaktadır. Türkiye'nin 2020, 2018, 2016 ve 2014 yıllarındaki sıralaması sırası ile 53, 53, 68 ve 71 biçimindedir.

Dünya ülkeleri tarafından yürütülen blokzincir çalışmalarına ilişkin yapılan literatür araştırması sonucunda 64 ülke ile Avrupa Birliği, Birleşmiş Milletler ve Dünya Bankası tarafından gerçekleştirilmiş olan 223 faaliyet tespit edilmiş olup bu çalışma sayılarının ülkelere göre dağılımı Çizelge 2.29'da verilmiştir. Buna göre, blokzincir teknolojisine ilişkin kamu uygulaması sayısı bakımından Amerika Birleşik Devletleri en önde gelmekte olup BM E-Devlet Gelişmişlik İndeksine göre ilk on sırada yer alan ülkeler ile ilk on dışındaki Birleşik Arap Emirlikleri, Kanada, Rusya, Çin, Almanya ve Malta'nın diğer ülkelere kıyasla daha fazla sayıda somut çalışmalar yürüttükleri görülmektedir.

Çizelge 2.29. Ülkeler ve uluslararası kuruluşlarca gerçekleştirilmiş olan blokzincir kamu uygulamalarının sayıları

Ülke	E-devlet Idx (2022)	Uyg. Sayı	Referans
Amerika Birleşik Devletleri	10	22	(Killmeyer ve diğerleri, 2017); (Shuaib, Daud, Alam ve Khan, 2020); (Richards, 2018); (Hill ve Foster, 2019); (Brainard, 2020); (Moore ve Sawhney, 2019); (USA Homeland Security Department, 2016); (Dewey, 2019, 2020).
Avustralya	7	17	(Killmeyer ve diğerleri, 2017); (Standards Australia, 2017); (Commonwealth of Australia, Department of the Prime Minister and Cabinet, 2015); (Richards, 2018); (Reeves, 2020: 251); (Ma, 2019); (Power Ledger, 2019a, 2019b); (Ramachandran ve Rehermann, 2019).
Birleşik Arap Emirlikleri	13	12	(Birleşik Arap Emirlikleri (BAE) Hükumeti, 2020a); (Beretta, 2019: 459); (BAE Hükumeti, 2020b); (Dubai Future Foundation, 2016); (Dubai Land Department, 2017)
Hollanda	9	12	(Schep ve diğerleri, 2019: 395); (Shuaib ve diğerleri, 2020); (Bhunia, 2018).
Rusya	42	11	(Shuaib ve diğerleri, 2020); (Kakushadze ve Liew, 2018); (Strizh, Dmitriev ve Kiseleva, 2020: 486); (Federal Antimonopoly Service of the Russian Federation, 2016); (Russian National Settlement Depository (NSD), 2018a); (ICT Moscow, 2020); (Russian National Settlement Depository (NSD), 2018b); (Russian National Settlement Depository (NSD), 2016)
Çin	43	10	(Dong, 2018); (Zhang, 2018); (Blacklock ve Lei, 2020: 316); (Houben ve Snyers, 2020); (Ledger Insights, 2020); (Chang, 2017); (GovChain, 2019b)
İngiltere	11	8	Walport (2016: 8); (Davis, Maxson ve Moyle, 2020)
Kanada	32	8	(Shuaib ve diğerleri, 2020); (Davradakis ve Santos, 2019); (Grant, Lim ve Peters, 2020: 294); (Ahmad, 2018); (British Columbia Eyaleti, 2020); (The University of British Columbia, 2017)
Estonya	8	7	(Killmeyer ve diğerleri, 2017); (Lätt, 2020: 332); (e-Estonia Briefing Centre, tarih yok)
Almanya	22	6	(Almanya Maliye Bakanlığı, 2019); (Davradakis ve Santos, 2019); (Fridgen, Guggenmos, Lockl, Rieger ve Urbach, 2019); (Almanya Ekonomik İşler ve Enerji Bakanlığı (BMWi), 2019)
Güney Kore	3	6	(Killmeyer ve diğerleri, 2017)
Avusturya	20	5	(Rath ve Kulnigg, 2020: 263); (Austrian Federal Computing Center (BRZ), 2020); (Avusturya Ticaret Odası, 2019)
Bahreyn	54	5	(GovChain, 2019a); (Bahrain Fintech Bay, 2017)
Malta	15	5	(Ministry for European Affairs and Equality, 2018); (Parliamentary Secretariat for Financial Services, Digital Economy and Innovation Office of the Prime Minister, 2018: 10); (Falzon ve Valenzia, 2019); (Office of the Prime Minister Malta, 2017); (Office of the Prime Minister Malta, 2018a); (Office of the Prime Minister Malta, 2018b); (Office of the Prime Minister Malta, 2019)
İsveç	5	4	(Kairos Future, 2017); (Houben ve Snyers, 2020); (Shuaib ve diğerleri, 2020)
İsviçre	23	4	(Procivis AG, 2019); (Gesley, 2018); (Lux ve Mathys, 2018); (Lux, 2019)
Japonya	14	4	(Smolenski, 2017: 25, 26); (Shuaib ve diğerleri, 2020)
Ukrayna	46	4	(Killmeyer ve diğerleri, 2017); (Shuaib ve diğerleri, 2020); (Bitfury, tarih yok); (Bitfury, 2017)
Arjantin	41	3	(Moreno ve Lomaquiz, 2020); (UN Economic Commission for Latin America and the Caribbean, 2019); (Blockchain Federal Argentina (BFA), 2018)

Ülke	E-devlet Idx (2022)	Uyg. Sayı	Referans
Avrupa Birliği	-	3	(Probst, Frideres, Cambier ve Martinez-Diaz, 2016); (DECODE, tarih yok); (Avrupa Komisyonu, 2017); (Perchet ve diğerleri, 2020); (Avrupa Komisyonu, 2018); (EU Blockchain Observatory and Forum, 2020); (The Law Library of Congress, Global Legal Research Center, 2018: 30); (Niforos, 2017: 35); (Merz, 2018); (Groenfeldt, 2017)
Fransa	19	3	(France Strategie, 2017); (Perchet ve diğerleri, 2020: 344); (Boring, 2018); (Houben ve Snyers, 2020)
Hong Kong	-	3	(ASTRI, 2016); (Hong Kong Legislative Council, 2017)
Lüksemburg	26	3	(Lüksemburg Standardizasyon, Akreditasyon ve Ürün ve Hizmet Kalitesi Enstitüsü (ILNAS) ve Standardizasyon ve Bilgi Ekonomisi Ajansı (ANEC), 2018); (INFRACHAIN, 2020); (Allessie ve diğerleri 2019); (Pascual, Holle ve Petit, 2020)
Malezya	53	3	(BERNAMA Media Relations and Event Management, 2019); (Min ve Yang, 2018); (LuxTag, 2019)
Norveç	17	3	(Ølnes ve Jansen, 2018)
Singapur	12	3	(Ciambella, Chong ve Lin, 2019: 420)
Şili	36	3	(Smartmatic, 2015); (ZIGURAT İnovasyon ve Teknoloji Okulu, 2019)
Yeni Zelanda	4	3	(Ojo ve Adebayo, 2017)
Birleşmiş Milletler	-	2	(World Food Programme, 2020); (Bacchi, 2017); (Fridgen ve diğerleri, 2018)
Brezilya	49	2	(Shuaib ve diğerleri, 2020); (Machado ve Abramof, 2020: 282); (Davradakis ve Santos, 2019); (Allison, 2017)
Danimarka	1	2	(Killmeyer ve diğerleri, 2017)
Finlandiya	2	2	(Fridgen ve diğerleri, 2018)
Gana	106	2	(Shuaib ve diğerleri, 2020); (Berryhill ve diğerleri, 2018).
İspanya	18	2	(López-Ibor, Stöger ve Jin, 2019: 438)
Barbados	79	1	(Moore ve Stephen, 2015)
Belarus	58	1	(Belarus Blockchain Association, tarih yok)
Belçika	39	1	(Port of Antwerp, 2017)
Çek Cumhuriyeti	45	1	(Czech Republic Blockchain Republic, tarih yok)
Dünya Bankası	-	1	(Ebert, 2019)
Güney Afrika	65	1	(Burbidge, 2016)
Gürcistan	60	1	(Pipan, 2017); (Shuaib ve diğerleri, 2020); (Shin, 2017)
Hindistan	105	1	(Shuaib ve diğerleri, 2020); (Ramanathan, Tiwari ve Rautray, 2019: 335)
Honduras	155	1	(Chavez-Dreyfuss, 2015)
İrlanda	30	1	(McLaughlin, Ryan ve Devlin, 2020)
İsrail	16	1	(Blockchain Israel, 2017)
İtalya	37	1	(Donna ve Di Maria, 2020)
Kamboçya	127	1	(Bangkok Post, 2020)
Katar	78	1	(Tasmu Digital Valley, 2019)
Kazakistan	28	1	(Abugaliyeva, 2018)
Kenya	113	1	(The World Bank, 2017)
Kuveyt	61	1	(The Law Library of Congress, Global Legal Research Center, 2018)
Letonya	29	1	(Avrupa Komisyonu, 2019)
Lihtenştayn	25	1	(Bank Frick, 2019)
Litvanya	24	1	(Bank of Lithuania, 2020)

Ülke	E-devlet Idx (2022)	Uyg. Sayı	Referans
Meksika	62	1	(C Minds, 2018)
Portekiz	38	1	(Marques ve Albuquerque, 2020)
Senegal	143	1	(Tobor, 2016)
Slovakya	47	1	(Blockchain Slovakia, 2017)
Slovenya	21	1	(Žarkovič, 2019)
Suudi Arabistan	31	1	(The Law Library of Congress, Global Legal Research Center, 2018)
Tayland	55	1	(Leesa-Nguansuk, 2017)
Tunus	88	1	(EconoTimes, 2016)
Uruguay	35	1	(Houben ve Snyers, 2020)
Venezuela	128	1	(Houben ve Snyers, 2020)
Yunanistan	33	1	(Siassiakos, Ilioudi, Effrosyni, Mitsiou ve Nanouris, 2020).
Toplam		**223**	

Dünya ülkelerinin yürüttükleri çalışmalar içerisinde proje konusu bakımından ilk üç sırayı blokzincir merkezinin kurulması, finansal hizmetler ve dijital kimlik (yetki belgeleri, lisanslar, sertifikalar) almakta, bunları dijital para birimi, blokzincir teknolojisinin kullanımına yönelik strateji belgesi ve gayrimenkul işlemleri izlemektedir. Dünya ülkelerindeki blokzincir konulu kamu faaliyetlerinin konularına göre dağılımları Çizelge 2.30'da verilmiştir.

Çizelge 2.30. Blokzincir konulu faaliyetlerin konularına göre dağılımları

Proje Tipi	Adet	Proje Tipi	Adet
Blokzincir Merkezi	28	Sosyal Yardımlar	4
Finansal Hizmetler	26	İhale/Satınalma Sistemi	3
Dijital Kimlik (Yetki Belgeleri/Lisanslar/Tasdikler)	25	Yazılım Yarışması	3
Dijital Para Birimi	19	Sibergüvenlik	3
Strateji/Araştırma	17	Sosyal Güvenlik	2
Gayrimenkul İşlemleri, Tapu Kaydı	16	Askeri savunma altyapısı	2
Tedarik Zinciri Yönetimi	11	Sadakat programı	1
Kişisel Kayıtlar (Sağlık, finans vb.)	11	Vergi Toplama	1
Elektronik Oylama	10	Denetim	1
Veri Toplama, Kayıt ve/veya Paylaşımı	7	Tahsilat	1
Enerji ticareti	5	Nesnelerin İnterneti (IoT)	1
Veri Piyasası/Veri Parasallaştırma	5	Blokzincir test ortamı	1
Blokzincir Altyapısı	5	Çevresel atık yönetimi	1
Ulaşım/Lojistik	4	i-Oyun	1
Kamu Kayıtları	4	Kriptopara Cüzdanı	1
Varlık Kaydı ve Yönetimi	4		
Toplam			**223**

Blokzincir uygulamalarının sektörlere göre dağılımda ise finansal hizmetler önemli bir farkla öne çıkmakta, finansal uygulamaları blokzincir faaliyetlerini tek çatı altında organize etmek, kamu ve özel sektör çalışmalarını konsolide ederek işbirliğini geliştirmek ve ortak bir altyapı ile rehberlik etmek üzere kurulan blokzincir araştırma merkezleri izlemektedir. Kamu tarafından yürütülen blokzincir faaliyetlerinin sektörel dağılımı Çizelge 2.31'de verilmiştir.

Çizelge 2.31. Dünyadan kamu blokzincir uygulamalarının sektörlere göre sayıları

Sektör	**Adet**	**Sektör**	**Adet**
Finansal Hizmetler	56	Sosyal Yardımlar	4
Kamu Hizmetleri - Araştırma Merkezi	28	Siber güvenlik	3
Strateji Geliştirme/Araştırma	20	Ulaştırma	3
Varlık (gayrimenkul, araç vb.) Kaydı ve Yönetimi	20	Çevre	2
Dijital Kimlik	18	Satınalma	2
Veri Yönetimi	14	Savunma Sanayii	2
Tedarik Zinciri Yönetimi	11	Sosyal Güvenlik Sistemi	2
Seçimler ve Oy kullanma	10	Gümrük İşlemleri	1
Enerji	7	Nesnelerin İnterneti (IoT)	1
Sağlık Hizmetleri	6	Noter hizmetleri	1
Eğitim	5	Oyun	1
Ağ - Altyapı	5	Sadakat Programı Yönetimi	1
Toplam			**223**

Çalışmalar, başlangıç tarihlerine göre sınıflandırıldığında 2012 yılından itibaren 2017 yılına kadar çalışma sayısının sürekli artış göstererek 2017 yılında en yüksek değere ulaştığı, daha sonra çalışma sayısının azalma eğilimi gösterdiği görülmektedir.

Tespit edilen kamu faaliyetlerinin içerisinde yer alan, doğrudan teknolojinin uygulanmasına yönelik olmayan faaliyetler (blokzincir altyapısı, blokzincir merkezi, blokzincir test ortamı, strateji/araştırma ve yazılım yarışması) listeden çıkarılarak gerçek hayat uygulamaları yeniden sıralandığında kamu uygulamaları içerisinde en fazla yer tutan konular aşağıdaki biçimdedir:

- Finansal hizmetler – 26 adet
- Dijital kimlik, yetki belgeleri, lisanslar ve sertifikalar – 25 adet
- Dijital para birimi – 19 adet
- Gayrimenkul işlemleri, tapu kaydı – 16 adet

- Tedarik zinciri yönetimi – 11 adet
- Kişisel kayıtlar (sağlık, finans vb.) – 11 adet
- Elektronik oylama – 10 adet
- Veri toplama, kayıt ve paylaşımı – 7 adet

Bu konuları sırasıyla veri parasallaştırma, enerji ticareti, ulaşım, sosyal yardımlar, kamu kayıtları, ihale/satınalma sistemi izlemektedir.

2.4. Türkiye'de Blokzincir Çalışmaları

2.4.1. Türkiye'de blokzincir ekosistemi

Blokzincir teknolojisi tüm dünyada olduğu gibi Türkiye'de de gerek özel gerekse kamu sektörü tarafından yakından takip edilmektedir. 2017 yılı Kasım ayında kamu ve özel kurum/kuruluşların ihtiyaçlarına istinaden, blokzincir teknolojilerinin altyapısı, kurulumu, güvenlik ve mahremiyet analizi, iş modelleri, kitle fonlama yaklaşımları ve muhtelif teknik detayları üzerine Ar-Ge faaliyetlerini icra etmek üzere, BİLGEM UEKAE Matematiksel ve Hesaplamalı Bilimler Biriminin altında Blokzincir Araştırma Laboratuvarı (*BZLab*) kurulmuştur. BZLab'ın amacı alanın önde gelen uzmanlarını bir araya getirerek işletmelerin bu teknolojiyi kullanma kapasitelerini geliştirmek, blokzincir teknolojisinin teknik özelliklerini ve sunduğu çözümleri araştırmak, tasarım ve geliştirme çözümleri sunmak, işbirliğini geliştirmek için blokzincir ağları kurmaktır (Blokzincir Araştırma Laboratuvarı, 2017).

Blokzincir teknolojisi alanında test çalışmaları yürüten önemli kurumların başında Bankalararası Kart Merkezi (BKM) gelmektedir. BKM tarafından Sorularla Blockchain, Blockchain 101, Belgem.io –Herkes İçin Blockchain, Paranın Serüveni, Keşif: Blockchain'in Sırları, Yalın Blokzincir, Blokzincirlerde Güvenlik ve Mahremiyet, Blokzincir Almanağı 2019: Dünyadan Blokzincir Gelişmeleri, 5 Soruda Blokzinciri başlıklı yayınlar çıkarılmış, blokzincir teknolojisinin ilk somut örneği olarak Bay Bay Nakit (BBN) adlı Hyperledger Fabric platformu üzerinde çalışan uygulama geliştirilerek şirket içinde kullanılmaya başlanmıştır. BKM tarafından geliştirilerek kullanılmaya başlanan ikinci

uygulama ise Ethereum tabanlı bir dijital eğitim sertifikası saklama uygulaması olan belgem.io'dur.

Türkiye'de blokzincir teknolojisi konusunda faaliyet yürüten bir diğer kuruluş Türkiye Bilişim Vakfı liderliğinde kurulmuş olan Türkiye Blokzincir Platformudur. Türkiye'de sürdürülebilir bir blokzincir ekosisteminin ve bir paylaşım platformunun oluşturulması amacıyla kurulan, kâr amacı gütmeyen platform eğitimler ve etkinlikler düzenlemekte, kitap ve raporlar yayınlamakta, web sitesi aracılığı ile içerik üretmekte, hem yurtiçi hem de yurtdışından ilgili taraflarla işbirliğinde bulunmaktadır. Platform bünyesinde Finans, Bankacılık ve Sigortacılık, Hukuk, Düzenlemeler ve Kamu İlişikleri, Üretim, Lojistik ve Ulaşım, Uluslararası ve Akademik İlişkiler, Sağlık, Teknoloji ve Enerji konularında çalışmalar yapmak üzere çalışma grupları kurulmuştur. Türkiye Blokzincir Platformu Çalışma Grupları tarafından kamuya açık olarak yayınlanmış olan raporlar: Ülke Genelinde Uygulanabilir Enerji Sektörü Blockchain Kullanım Alanları, Avantajlar ve Riskler (2021), Kripto Varlıkların Vergi - Muhasebe ve Denetim Yönünden İncelenmesi (2021), Enerji Sektöründe Blokzinciri Gelişmeleri (2021), Ülkemizde Blokzincirin Uluslararası Ticarette Kullanımına Yönelik Çalışma Raporu ve Politika Önerileri (2021), Akıllı Sözleşme (2021), Tedarik Zincirleri ve Uluslararası Ticaret için Blok Zinciri (2021), Vergi - Muhasebe ve Denetim Açısından Kriptoparaların İncelenmesi (2021), Kriptopara ve ICO (2020), KVKK ve Blokzinciri Teknolojisi (2019), Açık Veri (2019), Blokzinciri Teknolojisi Terminoloji Çalışması (2019), Blockchain İçin Kavramsal Mimari (2019), Dijital Kimlik (2019), Dünyada Blokzinciri Regülasyonları (2019), Tedarikçi Tanıma Platformu (2019) biçimindedir.

Blokzincir ekosisteminde en önemli yer tutan kurumların başında üniversiteler gelmektedir. Üniversiteler hem verilen eğitim ve yürütülen araştırma faaliyetleri ile teknik altyapı ve insan kaynağının sağlanması konusunda üstlendikleri rol, hem de bünyelerinde barındırdıkları özel merkezlerin araştırma ve geliştirme faaliyetlerinde kullanımıyla sağlayacakları kolaylaştırıcılık ve koordinasyon yetenekleri ile teknolojinin anlaşılması ve gelişimi konusunda önemli bir konumdadırlar.

Üniversitelerin üstlendikleri bu önemli rolün bir göstergesi olarak, 2021 yılı Şubat ayında İstanbul Aydın Üniversitesi Blokzincir Uygulama ve Araştırma Merkezi kurulmuştur. Blokzincir teknolojisinin gelişmesine katkıda bulunmak ve ihtiyaç duyulan nitelikli

personeli sağlamak vizyonu ile kurulmuş olan merkez blokzincir teknolojilerinin altyapısı, kurulumu, güvenlik ve mahremiyet analizi, iş modelleri, kitle fonlama yaklaşımları ve muhtelif teknik detayları üzerine Ar-Ge faaliyetleri yürütmekte, eğitim, yayın ve tanıtım faaliyetlerinde bulunmaktadır (İstanbul Aydın Üniversitesi Blokzincir Uygulama ve Araştırma Merkezi, 2021).

Boğaziçi Üniversitesi İşletme Bilişim Sistemleri Tezli ve Tezsiz Yüksek Lisans Programında yer alan Fintek konulu seçmeli ders kapsamında blokzincir teknolojisi konusuna yer verilmekte (Boğaziçi Üniversitesi İşletme Bilişim Sistemleri Programı, 2020) olup Bilgisayar Mühendisliği Bölümü'nde ilk olarak 2017 yılında açılmış olan 'Blockchain Programming' dersi 20202 yılı itibariyle verilmeye devam etmektedir (Boğaziçi Üniversitesi Bilgisayar Mühendisliği Bölümü, 2022). Medipol Üniversitesi ise 9 Şubat 2018 tarihinde '*Blockchain* (Blokzinciri) Teknolojisi, *Bitcoin* ve Kripto Paralar' ismiyle bir seçmeli dersin okutulacağını duyurmuştur (Medipol Üniversitesi, 2018). Hâlihazırda Medipol Üniversitesi İşletme ve Yönetim Bilimleri Fakültesi, Ekonomi ve Finans Programında isteğe bağlı seçmeli ders olarak '*Blockchain* (Blokzinciri) Teknolojisi, *Bitcoin* ve Kripto Paralar' dersi verilmektedir (Medipol Üniversitesi, 2022) . Hacettepe Üniversitesi Bilgisayar Mühendisliği Bölümünde seçmeli olarak 'Fundamentals of Blockchain' dersi verilmektedir (Hacettepe Üniversitesi, 2022). Muğla Sıtkı Koçman Üniversitesinde 2017 yılında Blok Zinciri Araştırma Grubu, Hacettepe Üniversitesinde 2018 yılında Blokzincir Laboratuvarı, Bahçeşehir Üniversitesi bünyesinde Blockchainİst Center adıyla bir araştırma merkezi kurulmuştur.

2.4.2. Mevcut düzenleme faaliyetleri

Türkiye'de blokzincir teknolojisinin yasal düzenleme çalışmaları dünya ülkelerine benzer biçimde, öncelikle Bitcoin konusunda yayınlanan uyarı ile başlamış, daha sonra üst politika belgelerinde yer alan genel ifadelerle blokzincire atıfta bulunulmuştur. Kripto paraların risklerine odaklanan ilk duyuruda ve basın bildirilerinde konu ile ilgili yasal bir düzenleme olmadığı, yapısı itibariyle kripto paraların düzenleme ve denetim bakımından ilgili kurumların görev sahasına girmediği vurgulanmaktadır. Her ne kadar konu özelinde bir düzenleme bulunmasa da, Hazine ve Maliye Bakanlığı, Sermaye Piyasası Kurumu ve Bankacılık Düzenleme ve Denetleme Kurumu kripto paralar konusunu yakından takip etmekte, mevcut düzenlemelere aykırılık teşkil eden durumlarda gerekli müdahaleleri

yapmaktadırlar. İlgili kurum ve kuruluşlarca yapılan mevzuat çalışmaları aşağıda detaylı biçimde verilmiştir.

T.C. Cumhurbaşkanlığı

T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı (2019a) tarafından yayınlanmış olan On Birinci Kalkınma Planının 249.5. maddesinde "blokzincir tabanlı dijital merkez bankası parasının uygulamaya konulacağı", 508.3. maddesinde "blokzincir uygulamalarının yaygınlanştırılmasını teminen ulaştırma ve gümrük hizmetlerinde gerekli hukuki ve fiziki altyapı çalışmalarının tamamlanacağı", 809.2. maddesinde ise "kamu hizmetlerinin iyileştirilmesinde büyük veri, bulut bilişim, mobil platformlar, nesnelerin interneti, yapay zekâ, blokzincir gibi yeni teknolojilerden faydalanılabilmesi için süreç ve teknolojik altyapı iyileştirmelerinin yapılacağı" belirtilmektedir.

T.C. Cumhurbaşkanlığı 2020 Yılı Yıllık Programı'nda (2019b), Kalkınma Planının 249. maddesinde yer alan "Uluslararası ticaret sisteminde kabul görecek alternatif para ve ödeme sistemleri geliştirilmesi amacıyla ülke işbirlikleri tesis edilecek ve çalışmalar sürdürülecektir" ifadesine atıfta bulunularak "Tedbir 249.5. Blokzincir tabanlı dijital merkez bankası parası uygulamaya konulacaktır" hedefine yer verilmiş, Türkiye Cumhuriyet Merkez Bankası (TCMB) ve TÜBİTAK sorumluluğunda Anlık Ödeme Sisteminin tasarım ve yazılım geliştirme aşamalarının tamamlanarak, test çalışmalarına başlanacağı belirtilmiştir.

Hazine ve Maliye Bakanlığı ile Strateji ve Bütçe Başkanlığınca (2020) hazırlanan 2021-2023 Orta Vadeli Program (OVP) 29 Eylül 2020 tarihli ve 3030 sayılı Cumhurbaşkanı Kararı ile onaylanarak yayınlanmıştır. OVP'nin Kamu Maliyesi başlıklı 4 üncü bölümünün Politika ve Tedbirler kısmında "Dijital olarak alınıp satılabilen ve transfer edilebilen, dijital bir değeri temsil eden sanal varlıklar kullanılarak yapılan işlemlerin vergilendirilmesine yönelik çalışmalar sürdürülecektir." ifadesine yer verilmiştir.

T.C. Cumhurbaşkanlığı 2021 Yılı Yıllık Programı'nda (2020) da aynı biçimde 249.5. sayılı Tedbir olarak aynı hedefe yer verilmiş, sorumlu ve işbirliği yapılacak kuruluşlara Hazine ve Maliye Bakanlığı ilave edilerek yürütülecek faaliyet ve proje "Anlık Ödeme Sisteminin yaygınlaştırılmasına yönelik katman servislerin geliştirilmesi kapsamında TR Karekod ile

ödeme akışları hizmete geçirilerek; Merkez Bankası Sayısal Parası (MBSP) projesinin konumlanmasına yönelik karar alınacaktır" biçiminde güncellenmiştir. T.C. Cumhurbaşkanlığı 2022 Yılı Yıllık Programı'nda (2021) yine 249.5 sayılı tedbir olarak aynı hedef yer almış, bu Programda ayrıca Tedbir 508.3 altında sorumlusu Ticaret Bakanlığı olarak belirlenmiş olan "Blokzincir uygulamalarının yaygınlaştırılmasını teminen ulaştırma ve gümrük hizmetlerinde gerekli hukuki ve fiziki altyapı çalışmaları tamamlanacaktır" hedefine de yer verilmiştir.

25 Ekim 2022 tarihinde onaylanarak yayımlanmış olan T.C. Cumhurbaşkanlığı 2023 Yılı Yıllık Programı'nda Tedbir 249.5 "Blokzincir tabanlı dijital merkez bankası parası uygulamaya konulacaktır" biçiminde yer almaya devam etmiş, ancak bu Programda bir önceki 508.3 tedbirine yer verilmemiştir. Bu programda Tedbir 809.2'de sorumlusu Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, diğer ilgili kuruluşlar Sanayi ve Teknoloji Bakanlığı, Bilgi Teknolojileri ve İletişim Kurumu Başkanlığı, TÜBİTAK, TÜRKSAT olmak üzere "Kamu hizmetlerinin iyileştirilmesinde büyük veri, bulut bilişim, mobil platformlar, nesnelerin interneti, yapay zekâ, blokzincir gibi yeni teknolojilerden faydalanılabilmesi için süreç ve teknolojik altyapı iyileştirmeleri yapılacaktır" ifadesine yer verilmiştir (T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, 2022).

Bankacılık Düzenleme ve Denetleme Kurumu (BDDK)

Türkiye'de Bitcoin konusunda yapılan ilk resmi açıklama BDDK tarafından yayınlanan basın açıklamasıdır. BDDK (2013) tarafından yayınlanan 2013/32 sayılı bu basın açıklamasında herhangi bir resmi ya da özel kuruluş tarafından ihraç edilmeyen ve karşılığı için güvence verilmeyen bir sanal para birimi olarak bilinen Bitcoin'in, mevcut yapısı ve işleyişi itibarıyla 6493 sayılı "Ödeme ve Menkul Kıymet Mutabakat Sistemleri, Ödeme Hizmetleri ve Elektronik Para Kuruluşları Hakkında Kanun kapsamında elektronik para olarak değerlendirilmediği, bu nedenle de gözetim ve denetiminin mümkün görülmediği ifadesine yer verilmiş, Bitcoin ve benzeri sanal paraların riskleri sayılarak kamuoyu bu risklere karşı uyarılmıştır.

BDDK Bankacılık ve Finansal Piyasalar dergisinde yayınlanmış olan makalelerinde Mete, Koy ve Ersoy (2019) yatırımcıların kripto para piyasasında oluşan fiyat balonlarına karşı dikkatili olmaları gerektiğini belirtmekte, bununla birlikte blokzincir sistemlerinin ve kripto

para piyasalarının, gelişmiş devletler tarafından getirilen düzenlemeler ve bazı büyük firmaların kendi kripto paralarını çıkarmaları gibi etkenlere bağlı olarak geçerliliklerinin ve toplum nezdinde kabullerinin artma eğiliminde olduğunu öne sürmektedir.

Sermaye Piyasası Kurulu (SPK)

SPK, 01.12.2017 tarihli "Sanal Paralara dayalı işlemler" konulu Türkiye Sermaye Piyasaları Birliği'ne (TSPB) hitaben düzenlendiği yazı ile sanal para birimleri ile ilgili ülkemizde bir düzenleme ve tanımlama bulunmadığını, Sermaye Piyasası Kanunu kapsamında yer alan türev araçlara dayanak teşkil edebilecek unsurlar içerisinde de sanal para birimlerinin bulunmadığını belirterek bu aşamada, müşterilere yönelik olarak sanal para birimlerine dayalı spot veya türev işlemler yapılmaması gerektiğini duyurmuştur.

27.09.2018 tarihli ve 2018/42 sayılı SPK bülteninin Duyuru ve İlke Kararları başlıklı bölümünde Kurul Karar Organının 27/09/2018 tarih ve 47/1102 sayılı Kararı Uyarınca yapılan Dijital Varlık (Token) Satışları (ICO) Hakkında Duyuru başlığı altında blokzincir teknolojisi kullanılarak gerçekleştirilen ve genellikle kripto para ya da token satışı olarak bilinen para toplama faaliyetlerinin SPK düzenleme ve gözetim alanı dışında kaldığı belirtilerek bu tip arzların risklerinden bahsedilmiştir. Aynı duyuruda ICO'ların spekülatif ve çok riskli yatırım araçları olduğu, ICO'arın yapıları itibariyle düzenleyici ve denetleyici kurumların görev ve yetki alanı dışında kaldıkları belirtilmektedir.

Kitle fonlaması faaliyetlerine ilişkin sermaye piyasası mevzuatı kapsamındaki usul ve esaslar için ikincil düzenleme çalışmaları devam etmekte olup bu faaliyetlerin kurulun görev sahasına girip girmediği her bir duruma göre farklılık gösterecektir. SPK tarafından herhangi bir düzenleme yapılmamış olsa bile, kitle fonlaması adı altında izinsiz gerçekleştirilen faaliyetlerle ilgili idari ve cezai tedbirler uygulanmaktadır. Nitekim, kripto para karşılığı nakit toplayan Sikke Yazılım A.Ş. adlı firma tarafından gerçekleştirilen faaliyetler incelenerek Türk Ceza Kanununun 157 ve 158 inci maddelerine aykırılık nedeni ile suç ihbarı yapılmasına karar verilmiştir.

Hazine Müsteşarlığı (Mülga)

Mülga Hazine Müsteşarlığı'nın 11.01.2018 tarihli ve 2018/01 sayılı basın açıklamasında "Ülkemizde yasal bir dayanağı olmayan kripto paralara ilişkin düzenlemelerin geliştirilmesi için bir çalışma grubunun oluşturulmasına karar verilmiştir" ifadesine yer verilerek kripto paraların riskleri sıralanmış, bu risklere yönelik olarak kamuoyu uyarılmıştır.

T.C. Hazine ve Maliye Bakanlığı

Mali Suçları Araştırma Kurulu (MASAK) Başkanlığı (2019) Şüpheli İşlem Bildirim Rehberi'nde (Sürüm 1.4) daha önceki sürümde (Sürüm 1.3) yer verilmiş olan "T-001-3.47: Müşteri hesaplarından bitcoin satan aracı kuruluşlara bitcoin alımına yönelik para transferi yapılması" olarak belirtilmiş olan şüpheli işlem ifadesi değiştirilerek Bitcoin yerine kripto para terimi kullanılmış, şüpheli işlem tanımı da "T-001-3.47: Müşteri hesaplarından kripto para alımı amacıyla yurtiçi ve yurtdışı kripto para borsalarına ya da gerçek veya tüzel kişi hesaplarına müşteri profiline uymayacak sıklık ve tutarda para transferi yapılması" olarak güncellenmiştir. Rehberin son sürümünde kripto paralara ilişkin bir madde ilavesi yapılarak "T-001-3.61: Kaynağı bilinmeyen veya şahsın mali profili ile uygun olmayan şekilde yapıldığından şüphelenilen kripto para satımı sonucunda müşteri hesaplarına transfer gelmesi" biçiminde yeni bir şüpheli işlem tanımlanmıştır. Bu tanımlar ışığında, kaynağı belirli olan ve işlem yapan kişinin profiline uygun olan kripto para transferleri MASAK tarafından şüpheli işlem olarak değerlendirilmemektedir.

Ardından, 1 Mayıs 2021 tarihli Resmî Gazete'de yayımlanarak yürürlüğe giren "Suç Gelirlerinin Aklanmasının ve Terörün Finansmanının Önlenmesine Dair Tedbirler Hakkında Yönetmelikte Değişiklik Yapılmasına Dair Yönetmelik" ile "5549 sayılı Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun"un uygulanmasında yükümlü olarak kabul edilenlerin arasına, kripto varlık hizmet sağlayıcılar eklenmiş, bu mevzuat değişikliğini takiben MASAK tarafından 18 Nisan 2022 tarihinde Kripto Varlık Hizmet Sağlayıcılar için Şüpheli İşlem Bildirim Rehberi yayınlanmıştır.

T.C. Sanayi ve Teknoloji Bakanlığı

T.C. Sanayi ve Teknoloji Bakanlığı (2019) tarafından 18 Eylül 2019'da yapılan sunumla paylaşılan 2023 Sanayi ve Teknoloji Stratejisinde blokzincir ve dağıtık defter teknolojileri 2020 yılı içinde odaklanılacak teknolojiler arasında gösterilmiştir. Belgenin 22-Ulusal Blokzincir Altyapısı başlıklı bölümünde teknolojinin önemine atıfta bulunularak ulusal blokzincir altyapısının geliştirilmesi ve böylelikle blokzincir tabanlı ağ oluşturulmasının teşvik edileceği, bu teknolojiye dayalı uygulama geliştirme yetkinliğinin oluşturulması için öncelikle kamu merkezli uygulamaların blokzincir altyapısına taşınabilir olanlarının tespit edilerek "Açık Kaynak Platformu" bünyesinde projelendirilmesinin sağlanacağı, tedarik zinciri, bankacılık, hukuki takip uygulamaları gibi yeni ve güvenli iş modeli ve süreçlerin testi için, geliştirilen blokzincir altyapısında test ortamı ve katılımcı kümesinin oluşturulacağı belirtilmektedir. Ayrıca, geliştirilecek blokzincir uygulamalarının mevzuata uyumluluk testlerinin yapılması için sanal mevzuat test alanı oluşturulması ve buradaki testleri tamamlayan girişimlerin sertifikalandırılarak yatırım almalarının desteklenmesinin hedeflendiği vurgulanmaktadır.

T.C. Ticaret Bakanlığı

T.C. Ticaret Bakanlığı, (2019) "İhracat Blokzincir Teknolojisiyle Hızlanacak" başlığı ile duyurduğu haberde ihracat ve ithalat işlemlerinin blokzincir teknolojisiyle gerçekleştirilmesini sağlayacak yeni bir sistem üzerinde çalışmalara başlandığını bildirmiştir. Bu çalışmalar kapsamında, 30 Aralık 2020 tarihinde yapılan tanıtım toplantısı ile DigiKamp Dijital Dönüşüm Yarışması duyurulmuş, yarışmaya ilişkin şartname Ticaret Bakanlığı (2020) DigiKamp web sitesinde yayınlanmıştır.

Bilgi Teknolojileri ve İletişim Kurumu (BTK)

BTK (2020) tarafından hazırlanarak bilgilendirici mahiyette yayınlanan raporda dijital paranın tarihçesi, kripto para teknolojisi, blokzincir, kripto paraların kullanım alanları ve dünyada ve Türkiye'deki durumu hakkında bilgi verilmektedir.

2.5. Türkiye Kamu Sektörü Hizmetleri ve Blokzincir Kullanım Potansiyeli

Birleşmiş Milletler tarafından birçok dış uzman, araştırmacı, kurum ve kuruluşların da desteği ile her iki yılda bir tüm üye ülkeleri kapsayan bir e-Devlet araştırması yapılmaktadır. Bu araştırmaların onbirincisi ve aynı zamanda sonuncusuna ait rapor 2022 yılında yayınlanmıştır. Raporda sunulan verilere göre Türkiye 0,7983 (2020 yılında 0,7718; 2018 yılında 0,7112; 2016 yılında 0,5900) e-Devlet Gelişim İndeksi ile 193 ülke içinde 48. sırada (2020 ve 2018'de 53; 2016'da 68. sıra) yer almaktadır. Türkiye'nin hemen üzerinde yer alan bazı ülkeler sırasıyla Slovakya, Ukrayna, Çek Cumhuriyeti, Hırvatistan, Çin ve Rusya'dır (Birleşmiş Milletler, 2022).

Birleşmiş Milletler 2022 e-Devlet araştırmasına (2022) göre Türkiye'nin e-Katılım İndeks değeri ise 0,7841 olup bu alanda da 193 ülke içerisinde 18. sırada (2020'de 23; 2018'de 37; 2016'da 60. sıra) yer almaktadır. Aynı raporda, Türkiye, Telekomünikasyon Altyapısı İndeksi (TII) bakımından 0,6626 puanla dünya ortalaması olan 0,5751'in üzerindedir.

E-Devlet Gelişim İndeksi bir devletin e-Devlet yapısını oluşturan üç unsurun bütünleşik bir yaklaşımla değerlendirilmesi sonucunda elde edilen bir gelişmişlik indeksidir. Bu üç unsur; iletişim altyapısının yeterliliği, bilgi ve iletişim teknolojilerini kullanacak ve geliştirecek insan kaynağının kabiliyetleri ve çevrim içi hizmet ve içeriklerin erişilebilirliğidir. Bu üç temel unsuru ifade eden göstergeler Telekomünikasyon Altyapısı İndeksi (ITU tarafından geliştirilmiştir), İnsan Sermayesi İndeksi (UNESCO tarafından geliştirilmiştir) ve bir anket yolu ile toplanan verilerden türetilen Çevrimiçi Hizmetler İndeksidir. Bu üç indeksin ağırlıklı ortalamaları kullanılarak e-Devlet Gelişim İndeksi hesaplanmaktadır (Birleşmiş Milletler, 2020: xx).

E-Katılım ise yönetişimin ve sürdürülebilir gelişimin ana unsurlarından ve temel taşlarından biridir. E-katılım vatandaşların devlet organlarıyla iletişimini güçlendiren, bilgi ve iletişim teknolojileri vasıtasıyla açık ve katılımcı bir yönetişim anlayışını ortaya koyan bir göstergedir (Birleşmiş Milletler, 2020: xxix).

Birleşmiş Milletler raporundan da görüleceği üzere, Türkiye son yıllarda hem e-Devlet gelişimi hem de e-katılım bakımlarından gelişim göstermiş olup devlet tarafından sunulan elektronik hizmetlerin hem sayısı hem de kapsamı sürekli olarak artmaktadır.

Bilgi teknolojileri konusunda ilerlemiş olan ülkeler arasında yeni teknolojilerin kamu hizmetlerinde kullanımı konusunda hem rekabet hem de işbirliğine dayalı çalışmalar yürütülmektedir. Yeni bir teknoloji olarak blokzincir teknolojisi de bu rekabet ve işbirliğinin önemli konularından biridir. Yürütülen çalışmalar sınıflandırıldığında, öncelikle teknolojiyi tanıma aşamasında bilgi ve vizyon sunan araştırma raporlarının hazırlandığı, daha sonra bu raporlara dayalı stratejiler geliştirildiği, bu stratejiler doğrultusunda da uygulama ve pilot çalışmalar yürütüldüğü görülmektedir. Bu ülkelerdeki kamu hizmetlerine yönelik çalışmalarda dikkat çeken bir diğer husus da özel sektör temsilcileri ile yapılan işbirliği faaliyetleridir. Özellikle blokzincir teknolojisi konusunda uluslararası alanda isim yapmış ve projeler geliştirmiş olan şirketlere ev sahipliği yapan ülkelerde kamu uygulamalarının da diğer ülkelere göre çok daha ileri düzeyde olduğu görülmektedir.

Türkiye kamu yapısının tutulduğu ve KAYSİS olarak adlandırılan Elektronik Kamu Bilgi Yönetim Sistemi'nden alınan verilere göre kamu kurum ve kuruluşları ile sundukları hizmetler sınıflandırılmış olup bu sınıflandırmaya göre Cumhurbaşkanlığı, 16 adet Bakanlık ve Bağımsız Düzenleyici ve Denetleyici Kurumlar tarafından sunulan toplam hizmet sayısı Ekim 2022 itibariyle 14 326'dır. Yerel Yönetim Kuruluşları, Diğer Kurum ve Kuruluşlar ve Hizmet Yönünden Yerinden Yönetim Kuruluşları başlıkları altında gruplandırılmış diğer kurumlarca verilen hizmetlerle birlikte bu rakam 15 313'e ulaşmaktadır. KAYSİS'ten alınan hizmet sayılarının ilgili kurumlara göre dağılımları çizelge 2.32'de verilmiştir.

Çizelge 2.32. Kamu kurumları tarafından verilen hizmet sayıları (KAYSİS – 29.10.2022)

Birim	Hizmet sayısı
T.C. Cumhurbaşkanlığı	537
Türkiye Büyük Millet Meclisi Başkanlığı	7
Adalet Bakanlığı	297
Aile ve Sosyal Hizmetler Bakanlığı	300
Aile, Çalışma ve Sosyal Hizmetler Bakanlığı	591
Çevre, Şehircilik ve İklim Değişikliği Bakanlığı	431
Dışişleri Bakanlığı	152
Enerji ve Tabii Kaynaklar Bakanlığı	1 664
Gençlik ve Spor Bakanlığı	224

Birim	Hizmet sayısı
Hazine ve Maliye Bakanlığı	2 071
İçişleri Bakanlığı	648
Kültür ve Turizm Bakanlığı	677
Milli Eğitim Bakanlığı	698
Milli Savunma Bakanlığı	102
Sağlık Bakanlığı	918
Sanayi ve Teknoloji Bakanlığı	488
Tarım ve Orman Bakanlığı	1 978
Ticaret Bakanlığı	643
Ulaştırma ve Altyapı Bakanlığı	1 721
Bağımsız/Düzenleyici Denetleyici Kurum ve Kuruluşlar	179
Toplam	**14 326**

KAYSİS sistemine girilmiş olan kamu hizmetlerinin, bu tez çalışmasında önerilmiş olan modelin ilk aşamasındaki kriterler dikkate alınarak blokzincir teknolojisine uygunlukları bakımından değerlendirilip pilot çalışma yapılması için seçilebilecek süreçlerin seçiminde bir havuz işlevi görebileceği değerlendirilmektedir.

2.5.1. e-Devlet kapısında sunulan hizmetler

e-Devlet Kapısı, kamu hizmetlerini vatandaşlara, işletmelere, kamu kurumlarına bilgi ve iletişim teknolojileriyle etkin ve verimli bir şekilde sunma amacıyla hazırlanmış olan, tüm kamu hizmetlerine tek bir noktadan erişim imkanı sağlayan büyük bir internet sitesidir. e-Devlet Kapısı'nın kurulması ve yönetilmesi görevi T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı tarafından yürütülmekte olup sistemin geliştirilmesi ve işletimi Türksat A.Ş. tarafından gerçekleştirilmektedir (Dijital Dönüşüm Ofisi Başkanlığı, 2020).

www.turkiye.gov.tr adresinden hizmet veren e-Devlet Kapısında 2022 yılı Ekim ayı itibariyle 61 047 133 kayıtlı kullanıcı bulunmakta, 917 kurum tarafından web sitesi üzerinden 6 884 hizmet verilmektedir. Sunulan mobil hizmet sayısı ise 3 780'dir. Oldukça aktif ve yoğun biçimde kullanılmakta olan e-Devlet kapısında en sık kullanılan hizmetler sırasıyla aşağıdaki biçimdedir:

- Sosyal Güvenlik Kurumu, SGK Tescil ve Hizmet Dökümü
- Aile ve Sosyal Hizmetler Bakanlığı, Sosyal Yardım Başvuru Hizmeti
- Aile ve Sosyal Hizmetler Bakanlığı, Sosyal Yardım Bilgileri Sorgulama
- Sosyal Güvenlik Kurumu, Normal Şartlarda Ne Zaman Emekli Olabilirim?

- Gelir İdaresi Başkanlığı, Vergi Borcu Sorgulama
- Adalet Bakanlığı, Dava Dosyası Sorgulama
- Türkiye Noterler Birliği, Adıma Tescilli Araç Sorgulama
- Aile ve Sosyal Hizmetler Bakanlığı, Sosyal ve Ekonomik Destek Hizmeti Ön Başvurusu
- Emniyet Genel Müdürlüğü, Araç Plakasına Yazılan Ceza Sorgulama
- Tapu ve Kadastro Genel Müdürlüğü, Tapu Bilgileri Sorgulama
- Adalet Bakanlığı, İcra Dosyası Sorgulama
- Bilgi Teknolojileri ve İletişim Kurumu, Mobil Hat Sorgulama
- Milli Savunma Bakanlığı, Askerlik Durum Belgesi Sorgulama
- Ulaştırma ve Altyapı Bakanlığı, Barkodlu Araç Muayene Raporu Sorgulama

KAYSİS kamu hizmet envanterinde yer alan ve e-Devlet kapısından sunulan binlerce hizmet dikkate alındığında, kamu tarafından sunulan hizmetlere ilişkin bir bilgi altyapısının olduğu görülmektedir.

Özellikle bilgi teknolojileri konusunda ilerlemiş olan dünya ülkeleri arasında, teknolojik gelişmelerin kamu hizmetlerinde kullanımı konusunda çalışmalar yapılmaktadır. Kamu hizmetlerinde blokzincirin kullanılabilir olduğu alanlar aşağıdaki biçimde gruplandırılabilir:

- Ulusal kimlik yönetim sistemleri (kimlik kartları, ehliyet, pasaport vb.)
- Vergi toplama ve kamu gelirlerinin izlenmesi
- Oy verme işlemleri
- Güvenli mali hizmetler, bankacılık işlemleri
- Sağlık hizmetleri
- Sosyal yardımların dağıtılması ve takibi
- Mülkiyet kayıtları ve mülkiyet transferinin izlenmesi (Tapu Kayıt Sistemi vb.)
- Gıda güvenliği
- Tedarik zinciri yönetimi

Bu alanlara ilişkin blokzincir kullanma gerekçesi, kullanım alanına ilişkin problemli noktalar ve blokzincirin katacağı değer Çizelge 2.33'te verilmiştir.

Çizelge 2.33. Blokzincirin potansiyel kullanım alanları ve katacağı değer

Uygulama Alanı	Gerekçe	Mevcut Problemli Noktalar	Blokzincirin katacağı değer
Kimlik Yönetimi (Killmeyer ve diğerleri (2017)	Dijital kimlik hem başlı başına bir blokzincir uygulama örneği, hem de blokzincir kullanılarak yapılacak diğer uygulamalar için bir kolaylaştırıcıdır. Dünya üzerindeki toplam nüfusunun yaklaşık beşte birinin yasal bir kimliği olmadığı düşünüldüğünde kimlik yönetimi konusunun ne denli önemli olduğu görülecektir Kimlik yönetimi sadece vatandaş kimliklerinin yönetimi için değil aynı zamanda yetki belgeleri, lisanslar, sürücü belgeleri, sertifikalar gibi birçok alanı da kapsamaktadır. Kimlik yönetimi süreci birden fazla kurum ve kuruluşu ve vatandaşları içeren çok taraflı bir süreçtir	• Farklı tasdik süreçleri, kimlik ve yetki belgelerinin çıkarılması için farklı giriş kapıları (yetkilendirilmiş birden fazla kurum-kuruluş) kamu sektörünü bu teknolojinin kullanımı konusunda çekingen davranmaya itmektedir • Kimlik, sertifika, yetki belgesi vb. belgelerin dijital olarak sunulması ve kullanılması ile ilgili standartlar ve düzenlemeler bulunmamaktadır	• Çok farklı varlık sınıflarının etkin biçimde alışveriş işlemini mümkün kılan, güvenli ve kendini yöneten kimlik • Hangi kimlik bilgilerinin hangi amaçlarla paylaşıldığı konusunda bireylerin kontrol sahibi olmaları • Birden fazla kurumun aynı veriye aynı biçimde erişebilme olanağı • Bilgilerin güvenilirliğinin ve güvenliğinin artması
Tapu Kayıtları (Killmeyer ve diğerleri (2017)	Tapular sadece gayrimenkul alanların haklarını korumakla kalmaz aynı zamanda birçok gelişmiş ülkede bir yatırım ve ekonomik büyüme aracı olarak da işlev görürler. Bu kayıtların benzersiz ve değiştirilemez biçimde blokzincirde tutulması ve kayıtlardaki değişikliklerin blokzincir ile doğrulanması sayesinde güvenilir kayıtlara sahip olunacak, sahipsiz yerler veya aynı yerde birden fazla hak sahibinin bulunduğu durumlar ortadan kaldırılacaktır.	• Tescil ve kayıt işlemleri kâğıda dayalı ve parçalı biçimdedir. Bu durum da işlemleri maliyetli, verimsiz ve illegal müdahaleye açık hale getirmektedir. • Parsellerin mevcudiyeti ve bununla ilişkili mülkiyet kayıtlarının belirlenmesi çok uzun zamandır süregelen bir problemdir. Uygun ve sistematik bir izlemenin yetersizliği, dijital kayıtların bulunmayışı kamu otoriteleri ve mülk sahiplerin tarafından neyin kime ait olduğunun kesin biçimde görülebilmesini engellemektedir. • Gayrimenkullerin değerlemesi konusunda farklı modeller kullanılabilmektedir • Alım-satım değerlerinin gösterilmesinde bir standart bulunmamaktadır. Değerlerin usulüne uygun biçimde gösterilmemesi sonucunda devletin vergi kaybı olmaktadır.	• Merkezi olmayan, standartlaştırılmış sistemle aracıların sayısı azaltılacak, işlem yapan tarafların kimliklerine dair güven artacak, süreç etkinliği artacak, süreç zamanı ve maliyeti düşecektir. • Mülkiyet haklarının blokzincir ile kaydedilmesi ile tapu sigortacıları tasarruf edebilecektir. • Tapu idaresi, maliye, belediyeler, bankalar gibi birden fazla kurum tarafından güvenilir veriye kolay erişim sağlanabilecektir.

Uygulama Alanı	Gerekçe	Mevcut Problemli Noktalar	Blokzincirin katacağı değer
Elektronik Oylama (Killmeyer ve diğerleri (2017)	Çok kritik ve meşruiyetinin garanti edilmesi gereken kamu fonksiyonu olan oy verme işlemleri için de aynı biçimde blokzincir güvenli bir biçimde kullanılabilir. Aynen diğer işlemlerde olduğu gibi vatandaşlar oylarını blokzincir ile kullanabilir, oylarının sayılıp sayılmadığını doğrulayabilir ve hatta seçim sonuçlarını onaylayabilir. Potansiyel çözümler güvenli dijital kimlik yönetimi, anonim oy kullanma, bireyselleştirilmiş oy pusulası süreçleri ve pusula dökümlerinin onaylanması işlemlerinin harmanlanması ile kullanılmaktadır.	• Oy verme işleminin maliyeti • Seçim sonuçlarına müdahale etmek için düzenlenen siber saldırı tehditlerinin artışı • Seçim sonuçlarının denetimi sürecinin merkezi olması nedeniyle şeffaflığın zayıf olması • Oylamaya katılmayanlar nedeniyle oylama iptalleri ya da verimsizlikleri	• Potansiyel maliyet tasarrufu • Güvenliğin ve denetlenebilirliğinin artırılması potansiyeli • Seçimlere katılım oranını artırma potansiyeli • Vatandaşların şeffaflık ihtiyaçlarının karşılanması • Genel seçimler dışında belediyelerin, derneklerin vb. kurum kuruluşların karar mekanizmasına üyelerini ve vatandaşlarını daha hızlı ve daha kolay dâhil edebilmeleri sonucunda artan güven, şeffaflık ve gelişen yönetişim
Kişisel kayıtlar (sağlık, sigorta, mali bilgiler vb.)	Kimlik başlığı altında bahsedilenlerin ötesinde, diğer kişisel kayıtlar blokzincirle yönetilebilir. Örneğin, bir ağ içerisinde ya da ülke çapında sağlık kayıtları tüm hastaneler tarafından erişilebilir ve birlikte çalışılabilir. Bu tip bir uygulamada devletler hastaların gizlilik haklarını dikkate almalı, hastalardan öncesinde rızaları alınmalı ve sonuç olarak hastalar kendi verilerini kontrol edebilmelidir.	• Dağınık ve mükerrer kayıtların tutulmasının yol açtığı verimsizlik • Veri güvenliğini sağlama maliyetinin büyüklüğü • Verilerin gizliliğinin korunması konusundaki endişe ve güvensizlikler	• Verilere kullanıcının izni doğrultusunda ilgili tüm taraflarca ulaşabilme imkânı, • Daha güvenilir veri ve bilgi sorgulama olanağı • Veri güvenliğini sağlamak için gereken yedekleme, sibergüvenlik önlemleri vb. maliyetlerde tasarruf
Sosyal yardımlar	Sosyal yardımlar, hak sahiplikleri ve yardım süreçleri önemli miktarda masraf ve uygunluk için kontrol gereklilikleri içermektedir. Sosyal güvenlik ve emeklilik ödemeleri, tıbbi yardımlar, ulusal ve uluslararası yardımlar gibi devlet programlarında blokzincir teknolojisinden muazzam derecede faydalanılabilir. Örneğin, akıllı sözleşmelerden yardım edilecek kişilerin seçilmesi, yardımların dağıtılması ve doğal afetlerden etkilenenlere yapılacak yardımlarda faydalanılabilir. Ayrıca, yardımların gerçekten ihtiyaç duyanlara iletildiğinden emin olunmasında kullanılabilmektedir.	• Sosyal yardımların dağıtılmasında şeffaflık endişeleri • İhtiyaç sahiplerinin kayıtlarının tam ve güncel olmaması nedeniyle yardımların istenen etkinlikte gerçekleştirilememesi • Yolsuzluk ve usulsüzlük riskleri • Yapılan yardımların amacı dışında kullanılması • Yardımların ulaştırılması için ödenen ek ücretler (havale vb.)	• Sosyal yardım konusunda hak sahiplerinin durumlarının izlenme kolaylığı • Yapılan yardımların nasıl kullanılacağını kontrol edebilme imkanı • Yardımların iletilmesinde üstlenilen finansal maliyetlerde azalma • Yolsuzluk ve usulsüzlüklerin engellenmesi

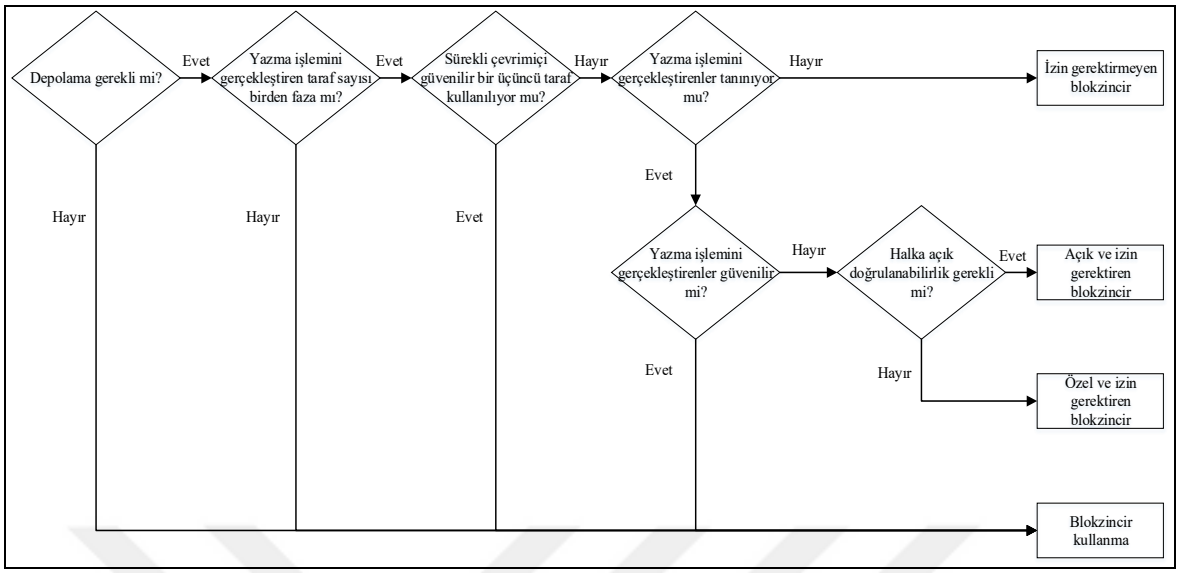
Uygulama Alanı	Gerekçe	Mevcut Problemli Noktalar	Blokzincirin katacağı değer
Telif hakları	Devletler genellikle telif haklarının kaydına müsaade etmekte veya telif hakları ile ilgili ihtilaflarla ilgili hakemlik etmektedirler. Konunun multidisipliner içeriği ve bazı durumlarda telif hakkının muğlaklığı nedeniyle blokzincir teknolojisinin sunduğu konu ile ilgili zaman damgasının tutulması, telif haklarının ihlalinin dikkatli biçimde izlenebilmesi ve zaman damgası içeren telif hakları sertifikalarının sağlanabilmesi fırsatları çok önemli bir araçtır. Bu bakımdan, blokzincir mevcudiyetin ve sahipliğin ispatı konusunda hizmet edebilmektedir.	• Gelişen teknolojiyle birlikte ihlallerin kolaylaşması ve artması • Özellikle elektronik ortamda üretilen ürünlerle ilgili hak sahipliği konusunda yaşanan ihtilaflar • İhlallerin tespitinde yaşanan güçlükler	• Sağladığı zaman damgası ile telif hakkı sahipliğini hızlı ve güvenilir biçimde ispatlama imkânı • Akıllı sözleşmeler ile eserlerin satışı, reklam ve telif hakkı yönetimi
Kripto Para	Blokzincirin ilk ve en yaygın kullanım alanıdır. Açık ve izin gerektirmeyen blokzincire dayalı kripto paralar herhangi bir otoriteye bağlı olmayan, mahremiyetin ve şeffaflığın korunduğu, yepyeni bir finansal sistem sunmaktadır.	• Paranın devletlerin kontrolünde olması, borç olarak arz edilmesi ve paranın sadece küçük bir bölümünün merkez bankalarınca çıkarılıp büyük bölümünün ticari bankalarca kredi-faiz ilişkisi ile dolaşıma sokulması • Merkezi otoriteye bağımlılık nedeniyle güvensiz olması • Para arzının neden olduğu enflasyon • Resmi kimlik belgesi olmadığı için finansal sisteme erişimi olmayan çok sayıda insan • Para transferlerinin yüksek maliyeti	• Tamamen merkeziyetsiz, şeffaf ve güvenli bir finansal sistem • Düşük işlem ücretleri • Finansal katılımın kolaylaştırılması • Yeni finansal pazarlar (DeFi)
Dijital Sertifika ve Diplomalar	Dijital sertifikalar ve diplomalar blokzincirin güvenlik ve şeffaflık özellikleri nedeniyle en yaygın biçimde kullanıldığı alanlardan biridir. Doğruluğunun kolaylıkla ispatlanabilmesi, sahtecilik ve tahrifat risklerini ortadan kaldırması, hazırlanması ve tesliminin çok kısa sürede tamamlanabilmesi gibi birçok avantaj ve kullanım kolaylığına sahiptir. Ayrıca, blokzincir teknolojisinin gerçek dünya uygulama örneğinin en fazla olduğu alanlardan biridir.	• Sahte ya da değiştirilmiş sertifika ya da diplomalara yaygın biçimde rastlanması • Taşıma ve saklama güçlüğü • Kaybedilmesi halinde yeniden çıkarılmasının zor ya da bazı durumlarda imkânsız olması • Doğruluğunun ve geçerliliğinin sorgulanmasının güçlüğü	• Herhangi bir aracı kuruma gerek olmadan doğrulanabilme • Güvenlik (kayıtları değiştirmek, ekleme ya da çıkarma yapmak çok daha zordur) • Hızlı ve kolay hazırlanabilme • Düşük maliyet

2.6. Blokzincirin Kullanılabilirliğinin Değerlendirmesi İçin Karar Modelleri

Blokzincir teknolojisinin herhangi bir alanda uygulanması için öncelikle cevaplanması gereken iki temel soru bulunmaktadır. Bunlardan ilki blokzincire gerçekten ihtiyaç olup olmadığı, ya da blokzincirin mevcut uygulamaya göre daha avantajlı olup olmadığıdır. Blokzincirin uygulanmasının gerçekten fayda sağlayacağı ve mevcut sisteme göre avantajlı olduğu değerlendirilirse bu kez ikinci soru gündeme gelmektedir: hangi tipte, hangi özelliklerde, nasıl bir blokzincir mimarisi en iyi çözümdür?

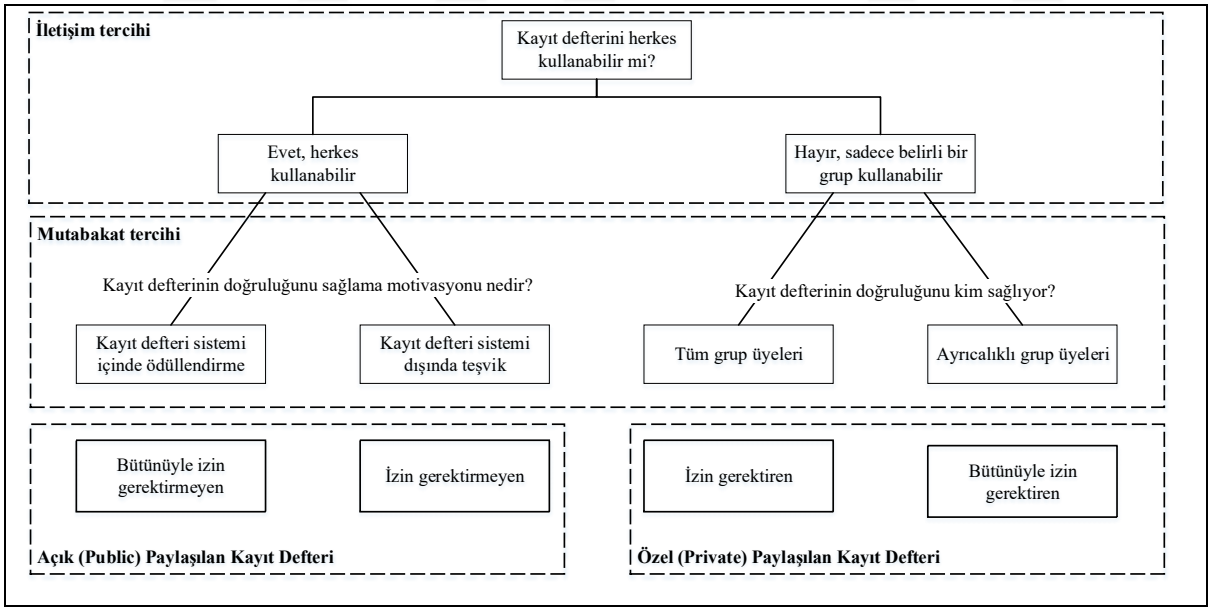
Blokzincirin kullanılabilirliğini değerlendirmek amacıyla literatürde çok miktarda çalışma bulunmaktadır. Bunlar genel itibariyle blokzincirin avantajlarını ve kısıtlılıklarını dikkate alarak geliştirilmiş karar ağaçları biçimindedir. Bu tez çalışması kapsamında geliştirilen modelin ilk adımında da benzer biçimde blokzincirin seçilen süreç için uygun olup olmadığı değerlendirilmektedir. Bu değerlendirme ve ilk karar noktası için literatürdeki çalışmalardan yeni bir karar ağacı hazırlanmasında faydalanılmıştır. Bu kapsamda incelenmiş olan çalışmalar aşağıda ilgili karar ağaçları ve akış şemaları ile birlikte sıralanmıştır.

Wüst ve Gervais (2018) çalışmalarında belirli bir uygulama senaryosu için blokzincir teknolojisinin uygun çözüm olup olmadığı konusunu izin gerektiren ve izin gerektirmeyen blokzincirler ile merkezi veritabanı seçeneklerini dikkate alarak analiz etmektedir. Açık ya da izin gerektiren blokzincirlerin kullanımı genel olarak, aralarında güven olmayan birden fazla sayıda kurumun etkileşim içinde bulunduğu, bir sistemin durumunda değişiklik yaptıkları ve bu işlemler için güvenilir bir üçüncü bir taraf üzerinde anlaşmaya gönüllü olmadıklarında anlamlıdır. Blokzincir çözümünün uygun olup olmadığı, uygun olması halinde hangi tip blokzincirin kullanılması gerektiğine dair karar verilmesinde kullanılması önerilen karar ağacı Şekil 2.9'da verilmiştir.



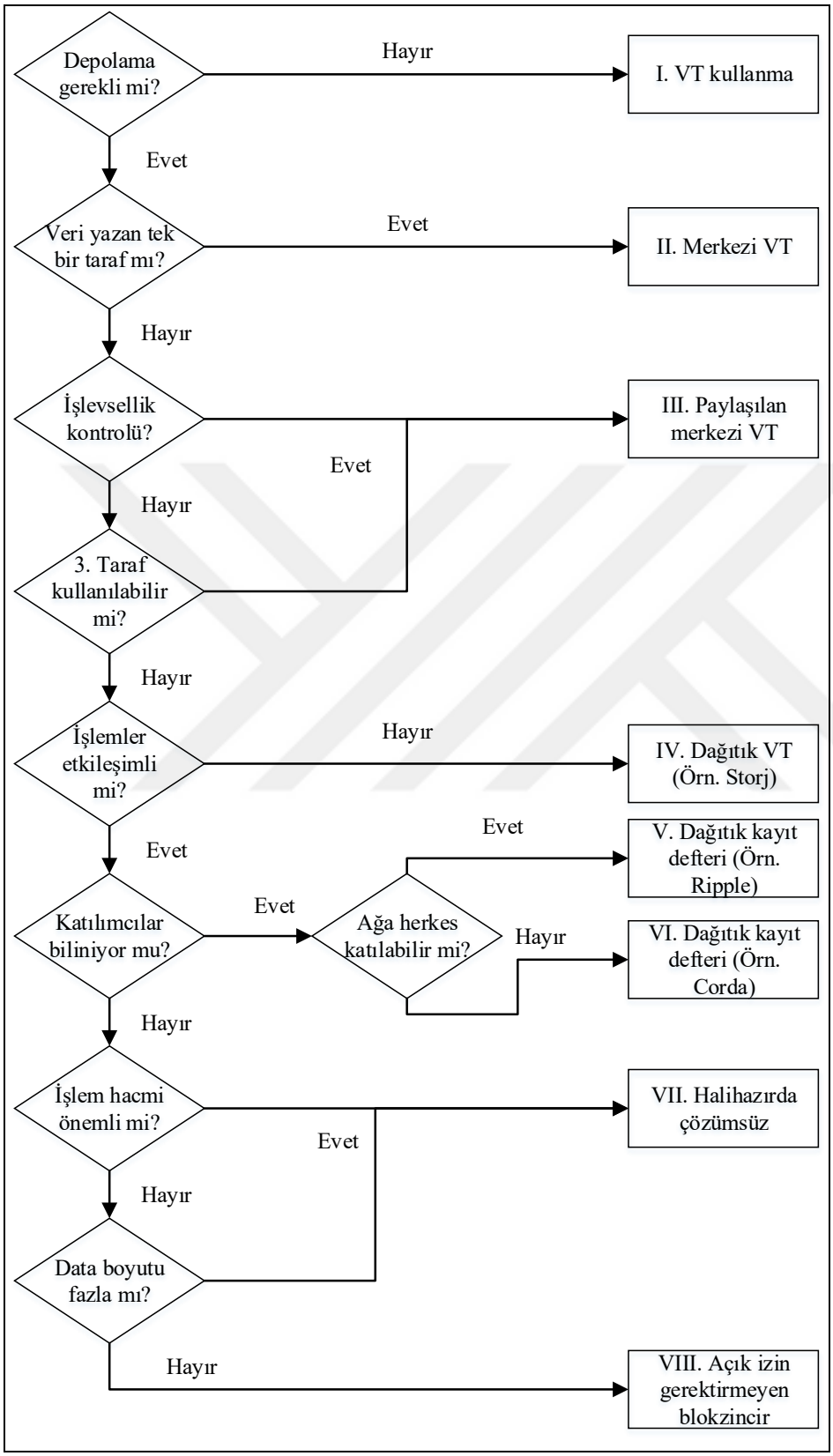
Şekil 2.9. Blokzincirin uygun çözüm olup olmadığına karar vermek için kullanılan akış şeması (Wüst ve Gervais, 2018).

Birch, Brown ve Parulava (2016) tarafından geliştirilmiş olan, izin gerektiren ve gerektirmeyen dağıtık kayıt defteri seçimine ilişkin model Şekil 2.10'da verilmiştir.



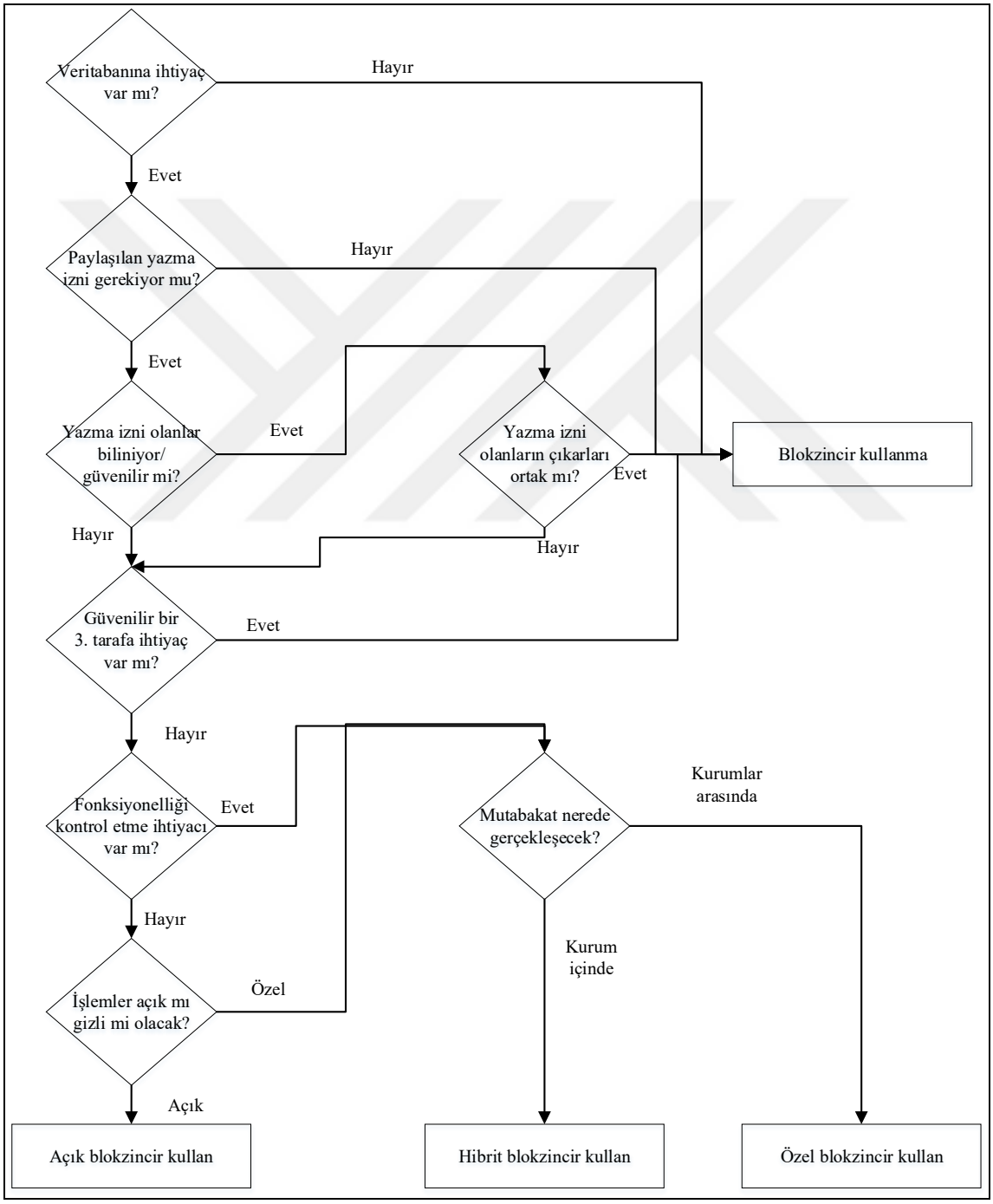
Şekil 2.10. Birch, Brown ve Parulava blokzincir seçim modeli.

Koens ve Poll (2018) yaptıkları çalışmada literatürdeki 30 farklı karar modelini inceleyerek veri tabanı, dağıtık kayıt defteri ve blokzincir teknolojisinin kullanımına ilişkin bir model geliştirmiştir. Bu model Şekil 2.11'de verilmiştir.



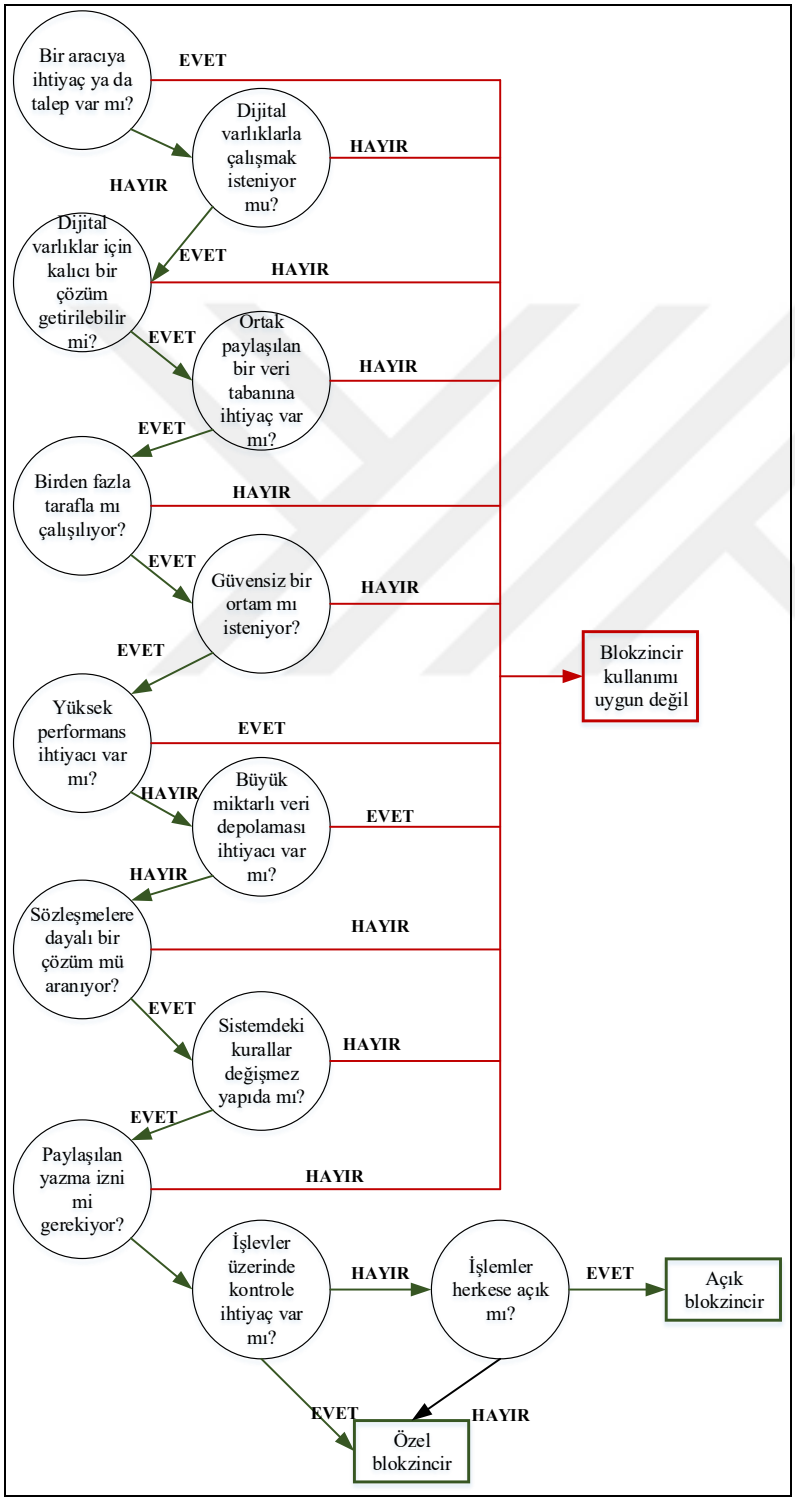
Şekil 2.11. Hangi tip veri tabanının uygun olduğunu belirlemek için bir model (Koens ve Poll, 2018).

Suichies (2015) blokzincir teknolojisinin kullanılması için bazı temel ilkelerin karşılanması gerektiğini ileri sürerek bu teknoloji uygulanmadan önce, gereksiz bir proje yürütmüş olmamak için blokzincirin gerekip gerekmediğinin iyi düşünülmesi gerektiğini belirtmektedir. Suichies tarafından blokzincire ihtiyaç duyulup duyulmadığı konusuna karar vermek için önerilen model Şekil 2.12'de verilmiştir.



Şekil 2.12. Blokzincir kullanımı için karar modeli, Suichies (2015).

Anwar (2018), blokzincir çözümüne ihtiyaç olup olmadığı kararı için 13 soruluk bir karar ağacı önermekte, modeldeki sorulara verilen "evet" ve "hayır" cevapları blokzincir çözümünün uygun olup olmadığı, uygunsa hangi tip blokzincir yapısının kullanılması gerektiği sonucuna götürmektedir. Bu karar ağacı Şekil 2.13'te verilmiştir.



Şekil 2.13. Blokzincir çözümünün uygunluğu için karar ağacı (Anwar, 2018).

Şekil 2.13'te verilen karar ağacına göre, sorulması gereken ilk soru bir aracıya ihtiyaç olup olmadığı, ya da bir aracının istenip istenmediğidir. Blokzincirin en cazip taraflarından biri aracılara olan ihtiyacı ortadan kaldırma potansiyelidir. Sistemlerdeki aracı ihtiyacı beraberinde ilave maliyet, bazı durumlarda artan işlem süresi ve güvenlik problemlerini beraberinde getirmektedir. Bu nedenle blokzincir çözümünün uygulanabilirliği değerlendirilirken ilk adımda bir aracının gerekli olup olmadığı, sistemde görev yapan aracıların ilave maliyet, zaman kaybı, veri güvenlik sorunları gibi olumsuzluklara yol açıp açmadıkları değerlenirilmelidir. Eğer bir aracı isteniyorsa blokzincir uygun çözüm değildir.

Karar ağacının ikinci adımında sistemde dijital varlıklarla çalışılıp çalışılmayacağına cevap aranmaktadır. Blokzincir teknolojisi ile birlikte ortaya çıkan dijital varlıklar temel olarak dört sınıfa ayrılmaktadır: kripto paralar (para tokenleri), varlık tokenleri, hizmet tokenleri (utility token) ve menkul kıymet tokenleri. Para tokenleri Bitcoin, Nano gibi ağlarda para birimi olarak kullanılan dijital varlıklar, varlık tokenleri DGX (DigixDAO Altın) gibi belirli veya fiziksel ürünleri temsil eden dijital varlıklar, hizmet tokenleri ETH (Ethereum) gibi, ağ içerisinde belirli haklara sahip olma ya da belirli faaliyetleri yürütme imkanı sağlayan dijital varlıklar, menkul kıymet tokenleri ise oy kullanma hakkı ya da şirket hissesi sağlayan, LSK (Lisk) gibi dijital varlıklardır. Bu dijital varlıklar blokzincir teknolojisi için zaruri olmamakla birlikte, teknolojinin getirdiği büyük bir güçtür. Eğer dijital varlıklarla çalışılmak isteniyorsa blokzincir teknolojisi kullanmak iyi bir seçimdir. Dijital varlıklar kullanılmayacak olsa bile blokzincir teknolojisi kullanılabilir ancak bu durumda başka çözümleri dikkate almak daha uygun olabilir.

Üçüncü soruda dijital varlıklar için kalıcı bir çözüm istenip istenmediği konusu değerlendirilmektedir. Bu soru ile kastedilen sistem içerisinde kaydedilen blokların, yani kayıt defterinin silinemez ve değiştirilemez olmasıdır. Eğer çözüm aranan süreçte veri değişikliği, güncelleme, silme ya da değiştirme gibi işlemler gerekiyorsa blokzincir teknolojisinin kullanımı uygun değildir.

Dördüncü soruda ortak paylaşılan bir veri tabanına ihtiyaç duyulup duyulmadığı sorulmaktadır. Aslında bu soru ilk sorudaki aracı kullanma istek ya da ihtiyacı ile yakından ilgilidir. Blokzincirde ağdaki diğer birçok tarafla ortak bir kayıt defterinin paylaşılması gerekir. Bu nedenle, çözüm aranan sistem için geleneksel bir veri tabanı yapısının özellikleri ile blokzincir teknolojisi kıyaslanarak en uygun olanına karar verilmelidir. Blokzincir

teknolojisinin geleneksel veri tabanlarına karşı üstün olduğu noktalar olduğu gibi daha zayıf olduğu konular da bulunmaktadır. Bu değerlendirme her bir sistem ya da çözüm aranan soruna göre farklılık gösterebilir.

Beşinci soru yapılan işte rol alan birden fazla tarafın olup olmadığıdır. Bir süreçte birden fazla tarafla birlikte çalışmak üst düzey güven, karşılıklı anlayış ve karmaşık işlem adımları gerektirir. Blokzincir teknolojisi bu tip bir ortamda süreci sorunsuz yönetmeyi mümkün kılar, tüm tarafların görebileceği bir kayıt defteri ile hem şeffaflığı sağlar hem de işlem sürelerini ve karmaşıklığı azaltabilir. Bu nedenle, süreçte rol alan taraf sayısı fazla ise blokzincir uygun çözüm olabilir.

Altıncı soru güvensiz bir ortam istenip istenmediğidir. Güvensiz ortamdan kasıt, üçüncü bir tarafa, aracılara, herhangi bir otoriteye güvenme zorunluluğu hissedilmeyen ortamdır. Geleneksel kurumlar tarafından tesis edilen güven, blokzincir teknolojisinde matematiksel ve kriptografik algoritmalarla, mutabakat mekanizması ile sağlanmaktadır. Bu soru aslında ilk soru ile ortak noktalar içermektedir.

Yedinci soruda yüksek performans gerekliliği sorgulanmaktadır. Blokzincir teknolojisinin en önemli eksikliklerinden biri performans yetersizliğidir. Bu sorunu gidermek için geliştirilen blokzincir platformları bulunmakla birlikte henüz yeteri kadar ilerleme kaydedilememiştir. Bu nedenle, eğer yüksek performanslı bir çözüm isteniyorsa blokzincir teknolojisi doğru seçenek olmayabilir. Performansı etkileyen unsurlardan biri ağ yapısının karmaşıklığıdır. Açık blokzincir platformunun etkinliği ve gücü ağdaki düğüm sayısının fazlalığına bağlıdır. Bu fazlalık da güvenliği artırırken performansı düşürmektedir. Performansla ilgili son özellik ise hızdır. Açık blokzincirlerde hız geleneksel veri tabanı sistemlerinin çok gerisindedir. Ancak, özellikle son zamanlarda blokzincirdeki performans ve ölçeklenebilirlik problemlerine çözüm getiren ve İkinci Bölüm'de yer verilen bazı blokzincir platformları geliştirilmiştir. Bu nedenle, bu çalışmada, Anwar (2018) tarafından önerilen modeldeki bu soruya ilişkin değerlendirme, yani performans gerektiren çözümler için blokzincirin uygun olmadığı sonucu revize edilmiştir.

Sekizinci soru büyük depolama birimlerinin gerekip gerekmediğidir. Blokzincir teknolojisi büyük miktarda veri depolama için genellikle uygun bir çözüm değildir. Ancak büyük veri

için geliştirilmiş olan ve İkinci Bölümde özelliklerine yer verilen BigChainDB gibi blokzincir platformları bulunmaktadır

Dokuzuncu soruda, sözleşmelere dayalı bir çözüm aranıp aranmadığı sorulmaktadır. Akıllı sözleşmelerin kullanımı zaruri ise, ya da kullanılmasının avantaj sağlayacağı düşünülüyorsa blokzincir teknolojisi kullanılmalıdır.

Onuncu soru, sistemdeki kuralların değişiklik gerektirmemesi ya da çok küçük değişiklik gerektirmesine ilişkindir. Blokzincir sistemi merkezi olmayan bir yapıda olduğundan kuralların hiçbir güç tarafından değiştirilememesi istenen bir durumdur.

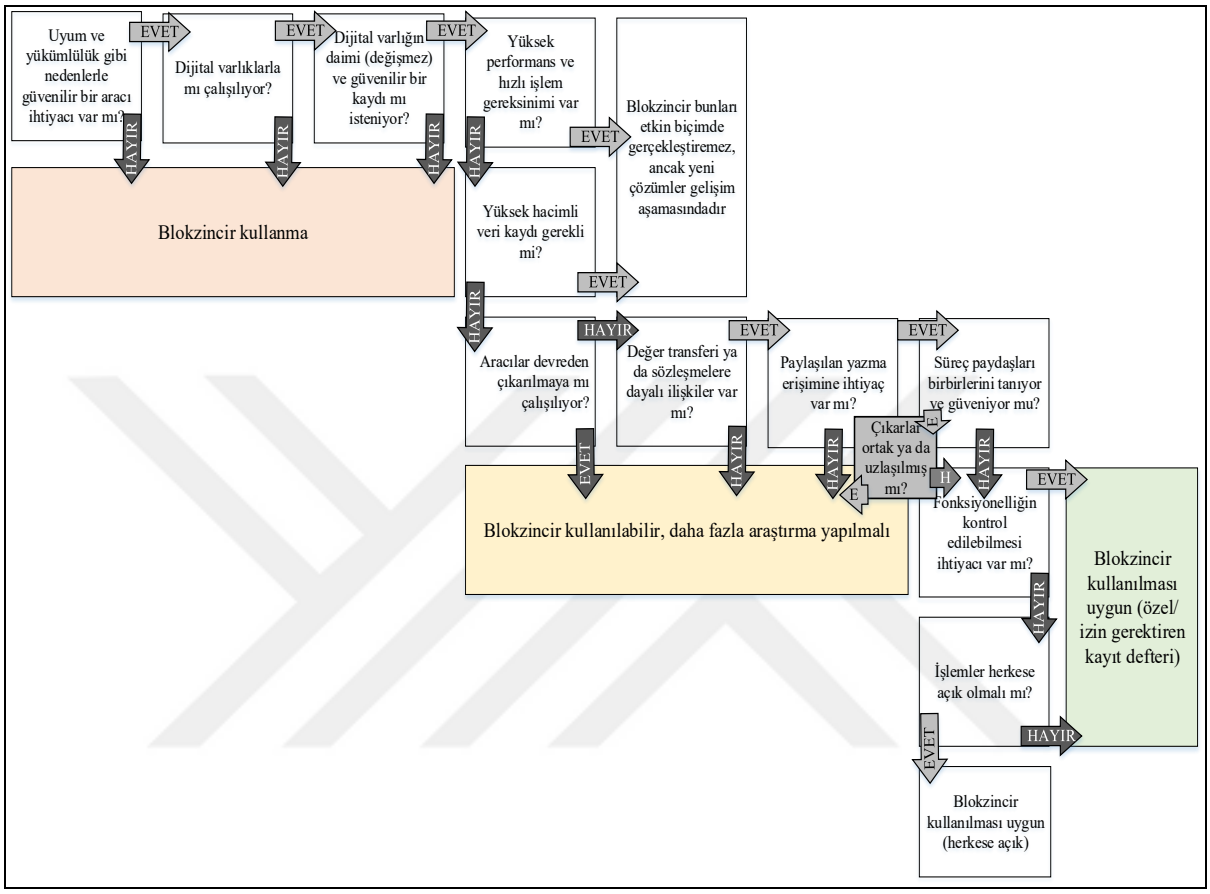
Onbirinci soruda, paylaşılan bir yazma iznine gerek duyulup duyulmadığı sorulmaktadır. Blokzincir yapısında ağdaki üyeler yazma ve okuma erişimi iznine sahiptir, ancak daha sonra bu kayıtları düzenleme ya da değiştirme yetkisinde sahip değildir. Bu soruya verilen evet cevabı ile artık blokzincirin uygun çözüm olduğu kararı verilir. Bu adımdan sonraki sorular blokzincirin herkese açık mı yoksa özel yapıda mı olması gerektiğine ilişkindir.

Onikinci soru işlevler üzerinde kontrol ihtiyacı olup olmadığıdır. Özel blokzincir ağında ağa erişmek izne tabidir. Açık ve özel blokzincir arasındaki temel fark kullanıcılar üzerindeki kontroldür. Özel blokzincirde onay mekanizmasına kimin katılabileceğine, kayıt defterini kimlerin sağlayabileceğine, kimlerin karar ve oy verme yetkisinin olacağına blokzincirin sahibi ya da yöneticisi karar verir. Bu yönü ile özel blokzincir merkeziyetsiz değil dağıtılmış bir kayıt defteridir. Eğer işlevler üzerinde kontrol isteniyorsa özel blokzincir yapısı tercih edilmelidir.

Son olarak ise işlemlerin herkese açık olmasının istenip istenmediği sorulmaktadır. Eğer herkese açık, tamamen şeffaf bir sistem isteniyorsa açık blokzincir, belirli yetkilendirmelere göre erişim izinleri verilmek isteniyorsa özel blokzincir seçilmelidir.

Mulligan da (2018) benzer biçimde, blokzincir teknolojisinin uygun çözüm olup olmadığına karar vermek için 11 sorudan oluşan Şekil 2.14'te verilmiş olan karar modelini önermiştir. Bu modelde sistemde aracı bulunup bulunmaması, dijital varlık kullanımı, kayıtların değiştirilememesi, performans gereksinimi, saklanacak datanın boyutu, akıllı sözleşmeler, paylaşılan yazma izinleri ve sistemdeki taraflar arasındaki güven durumu konularına ilişkin

sorular belirlenmiş, soruların yanıtlarına göre blokzincir çözümünün uygun olup olmadığı ya da karar vermek için daha ileri araştırmalar yapılması gerektiği çıktılarını veren bir akış şeması oluşturulmuştur.



Şekil 2.14. Blokzincir çözümü uygunluğu için karar modeli (Mulligan, 2018)

Geliştirilmiş olan bu karar ağaçlarından, önceki bölümlerde detaylı biçimde açıklanmış olan blokzincir özellikleri ile birlikte değerlendirilerek önerilen model kapsamında blokzincirin kullanılabilirlik kararı için kullanılacak karar ağacının hazırlanmasında faydalanılmaktadır.

2.7. Çok Kriterli Karar Verme (ÇKKV) Metotları

Karar vermede bilimsel bir süreç izlenmesi verilen kararın tutarlılığı ve kalitesini artırırken verilen kararın amaca uygunluğunu da sağlamaktadır. Karar verme için kullanılan birçok yöntem bulunmakta, problemin çeşidi ve karar verilecek olan konunun özelliklerine göre bu yöntemlerin her birinin avantajlı ve dezavantajlı olduğu taraflar bulunmaktadır.

Blokzincir teknolojisi temel felsefesi ve temel teknik özellikleri bakımından genel bir kavram olmakla birlikte, farklı tipte problemlere getirilen farklı çözümler içermesi nedeniyle kendi içerisinde birçok kriter ve çözüm alternatifini barındırmaktadır. Bu çalışmanın konusunu oluşturan blokzincir çözümünün seçiminde de bu nedenle iki aşamalı bir karar süreci söz konusudur. İlk aşamada blokzincir çözümünün tanımlanan problem için uygun olup olmadığına karar verilmektedir. Blokzincir teknolojisi birçok avantaj ve yenilik sunmakla birlikte her sürece uygulanabilecek jenerik bir çözüm değildir. Bu nedenle, öncelikle uygulanacağı alana uygun olup olmadığına karar verilmesi gerekmektedir. İlk aşamadaki bu seçim nispeten karar vermesi daha kolay, basit karar ağaçları ya da kontrol listeleri yardımı ile karar verilebilecek bir seçimdir. Ancak, blokzincir teknolojisinin uygun bir çözüm olduğu durumlarda blokzincirin hangi tasarımının ya da mimarisinin kullanılması gerektiği daha karmaşık bir problemdir. Bu nedenle, önerilecek blokzincir tasarımına en uygun biçimde karar vermek için Çok Kriterli Karar Verme metotlarından faydalanılması gerekmektedir.

Çok Kriterli Karar Verme problemi olarak ele alınan blokzincir çözümü seçiminde iki karar noktası dikkate alınmaktadır: kriterlerin belirlenerek bu kriterler için ağırlıkların belirlenmesi, bu kriterleri karşılayan alternatiflerin en uygun olandan en az uygun olana doğru sıralanması. Aşağıda ağırlıkların belirlenmesi ve alternatiflerin seçilmesi için kullanılabilecek yöntemler kısaca açıklanmaktadır.

2.7.1. Ağırlıklandırılmış Toplam Modeli (The Weighted Sum Model)

Uygulanması ve anlaşılması kolay, kullanımı basit olduğundan en yaygın biçimde kullanılan ÇKKV metotlarından biridir. Belirlenen kriterlere göre alternatiflerin performans değerlerinin ağırlıklı toplamlarının bulunarak bu toplam değerlerinin en büyük olanının en iyi alternatif olarak seçilmesine dayanmaktadır.

Genellikle tek boyutlu karar verme problemlerinde kullanılan bu modele göre m adet alternatif ve n adet kriter için en iyi alternatif Eş. 2.1'de verilmiş olan formüle göre hesaplanmaktadır (Windarto ve Muhammad, 2017).

$$A_i^{ATMSkoru} = \sum_{j=1}^{n} w_j a_{ij} \ , i = 1,2,3, \dots, m \tag{2.1}$$

Eş. 2.1'de 'n' kriter sayısını, 'm' alternatif sayısını, 'w' kriterlerin ağırlığını, 'a' ise ilgili alternatifin ilgili kritere göre değerini ifade etmektedir.

Ağırlıklandırılmış Toplam Modelini (ATM) bir örnek üzerinden ele almak üzere aşağıda işlem adımları verilmiş olan bir blokzincir platformunun seçimi süreci kurgulanmıştır. Bu örneğe göre, kullanım senaryosuna uygun beş blokzincir platformu arasından en iyisinin seçilmesi için işlem hacmi (saniyede işlem sayısı), işlem hızı (işlemin sonlanması için gereken bekleme süresi), olgunluk düzeyi (1 ile 5 arasında derecelendirme) ve popülarite (1 ile 5 arasında derecelendirme) kriterleri değerlendirilmektedir. Her bir platform için ilgili kriter değerleri platform özellikleri tablolarından alınmaktadır.

ATM'nin ilk adımında alternatif ve kriterlere göre eldeki veri setine göre Çizelge 2.34'te verilmiş olan temel tablo oluşturulmaktadır.

Çizelge 2.34. Her bir alternatif için ilgili kriter değerleri ve kriter ağırlıkları – ATM

Kriter	**İşlem hacmi (saniyede işlem)**	**İşlem hızı (saniye)**	**Olgunluk düzeyi (1-5 aralığında)**	**Popülarite (1-5 aralığında)**
Ağırlık / Alternatif	**0,3**	**0,2**	**0,25**	**0,25**
Ethereum	20	15	5	5
Hyperledger Fabric	3 500	1	3	4
Quorum	1 000	1	3	3
Corda	20 000	1	3	2
IOTA	10 000	12	2	3

Bu örnekte verilmiş olan ağırlık değerleri sübjektif değerler olup kriterin kullanım senaryosuna göre önemini ifade etmektir. Burada, işlem hacmi diğer kriterlere göre daha önemlidir. Her bir kullanım senaryosuna göre ağırlıklar ayrı biçimde derecelendirilmektedir.

Çizelge 2.34'te dikkat edilmesi gereken konulardan biri işlem hacmi, olgunluk düzeyi ve popülarite için maksimum değerlerin, işlem hızı için ise minimum değerin isteniyor oluşudur. ÇKKV problemlerinde kriterlerin bu özelliği fayda ve maliyet özelliği olarak adlandırılmaktadır. Bu durumda, bir sonraki adımda gerçekleştirilecek olan normalizasyon işleminde faydalı ya da maksimum değerli olması istenen nitelikler için her bir sütun değeri o sütunun maksimum değerine bölünürken ($X = x/x_{maks}$), faydasız ya da minimum değerli olması istenen nitelikler için o sütunun minimum değeri her bir sütun değerine

bölünmektedir ($X = x_{min}/x$). Bu işlemin ilk adımı olan maksimum (fayda kriterleri için) ve minimum (maliyet kriteri için) değerler Çizelge 2.35'te verilmiştir.

Çizelge 2.35. Her bir kriter için maksimum ya da minimum değerler – ATM

Kriter	İşlem hacmi (saniyede işlem)	İşlem hızı (saniye)	Olgunluk düzeyi (1-5 aralığında)	Popülarite (1-5 aralığında)
Ağırlık / Alternatif	**0,3**	**0,2**	**0,25**	**0,25**
Ethereum	20	15	**5 (maks)**	**5 (maks)**
Hyperledger Fabric	3 500	**1 (min)**	3	4
Quorum	1 000	1	3	3
Corda	**20 000 (maks)**	1	3	2
IOTA	10 000	12	2	3

Çizelge 2.35'te yüksek değerli olması istenen kriterler için sütun maksimum değerleri, düşük değerli olması istenen kriter için de sütun minimum değeri koyu renkte gösterilmiştir. Bu adımda bu maksimum ve minimum değerler kullanılarak normalizasyon işlemi gerçekleştirilmektedir. Bu işlem Çizelge 2.36'da verilmiştir.

Çizelge 2.36. Normalizasyon işlemi – ATM

Kriter	İşlem hacmi (saniyede işlem)	İşlem hızı (saniye)	Olgunluk düzeyi (1-5 aralığında)	Popülarite (1-5 aralığında)
Ağırlık / Alternatif	**0,3**	**0,2**	**0,25**	**0,25**
Ethereum	20/20 000	1/15	5/5	5/5
Hyperledger Fabric	3 500/20 000	1/1	3/5	4/5
Quorum	1 000/20 000	1/1	3/5	3/5
Corda	20 000/20 000	1/1	3/5	2/5
IOTA	10 000/20 000	1/12	2/5	3/5

Çizelge 2.36'da verilmiş olan normalizasyon işlemleri yapıldıktan sonra elde edilen normalize edilmiş karar matrisi Çizelge 2.37'de gösterilmiştir.

Çizelge 2.37. Normalize edilmiş karar matrisi – ATM

Kriter	İşlem hacmi (saniyede işlem)	İşlem hızı (saniye)	Olgunluk düzeyi (1-5 aralığında)	Popülarite (1-5 aralığında)
Ağırlık / Alternatif	**0,3**	**0,2**	**0,25**	**0,25**
Ethereum	0,001	0,067	1	1
Hyperledger Fabric	0,175	1	0,6	0,8
Quorum	0,05	1	0,6	0,6
Corda	1	1	0,6	0,4
IOTA	0,5	0,083	0,4	0,6

Sonraki adımda, her bir alternatifin her bir kritere karşılık gelen değeri ilgili ağırlık değeri ile çarpılmaktadır. Bu çarpım işleminden sonra ise her bir satır toplanarak her bir alternatifin performans puanı bulunmaktadır. Ağırlık değerleri ile çarpım sonucunda oluşan matris her bir alternatifin puanı ile birlikte Çizelge 2.38'de verilmiştir.

Çizelge 2.38. Her bir kritere göre alternatif değerlerinin ağırlıklarla çarpımı – ATM

Kriter	İşlem hacmi (saniyede işlem)	İşlem hızı (saniye)	Olgunluk düzeyi (1-5 aralığında)	Popülarite (1-5 aralığında)	Puan
Ağırlık / Alternatif	**0,3**	**0,2**	**0,25**	**0,25**	
Ethereum	0,0003	0,013333333	0,25	0,25	0,513633
Hyperledger Fabric	0,0525	0,2	0,15	0,2	0,6025
Quorum	0,015	0,2	0,15	0,15	0,515
Corda	0,3	0,2	0,15	0,1	**0,75**
IOTA	0,15	0,016666667	0,1	0,15	0,416667

Puan değerleri hesaplandıktan sonra alternatifler yüksek puandan aşağı doğru sıralanır. Çizelge 2.380'de verilmiş olan puanlara göre en iyi alternatif 0,75 puanla Corda'dır. Corda'yı sırasıyla Hyperledger Fabric, Quorum, Ethereum ve IOTA takip etmektedir.

2.7.2. Ağırlıklandırılmış Çarpım Modeli (The Weighted Product Model)

Ağırlıklandırılmış Çarpım Modeli (AÇM) Ağırlıklandırılmış Toplam Modeline oldukça benzemektedir. Aynı biçimde, bu model de belirlenen kriterlere göre alternatiflerin performans değerleri bulunarak değerlerinin en büyük olanının en iyi alternatif olarak seçilmesine dayanmaktadır.

Bu modele göre 'm' adet alternatif ve 'n' adet kriter için en iyi alternatif Eş. 2.2'de verilmiş olan formüle göre hesaplanmaktadır (Windarto ve Muhammad, 2017).

$$A_i^{AÇMSkoru} = \prod_{j=1}^{n} x_{ij}^{w_i} \ , i = 1,2,3, \dots, m \qquad (2.2)$$

Eş. 2.2'de 'n' kriter sayısını, 'm' alternatif sayısını, "w" kriterlerin ağırlığını ifade etmektedir. Bu formüle göre, her bir alternatif için, Ağırlıklandırılmış Toplam Modelinde açıklanmış olan normalize edilmiş kriter değerlerinin ağırlık değeri kadar üssü alınmakta, daha sonra bu değerler birbirleri ile çarpılarak ilgili alternatifin puanı hesaplanmaktadır.

Ağırlıklandırılmış Çarpım Modelinin işlem adımları Ağırlıklandırılmış Toplam Modelinde verilmiş olan örnek kullanılarak aşağıda verilmiştir. Buna göre, normalizasyon işlemine kadar aynı adımlar takip edildikten sonra, ağırlıklandırılmış çarpım değerlerinin hesaplanması için kullanılacak matris Çizelge 2.39'da verilmiştir.

Çizelge 2.39. Ağırlıklandırılmış Çarpım Modeli için normalize edilmiş karar matrisi

Kriter	**İşlem hacmi (saniyede işlem)**	**İşlem hızı (saniye)**	**Olgunluk düzeyi (1-5 aralığında)**	**Popülarite (1-5 aralığında)**
Ağırlık / Alternatif	**0,3**	**0,2**	**0,25**	**0,25**
Ethereum	$0{,}001^{0,3}$	$0{,}067^{0,2}$	$1^{0,25}$	$1^{0,25}$
Hyperledger Fabric	$0{,}175^{0,3}$	$1^{0,2}$	$0{,}6^{0,25}$	$0{,}8^{0,25}$
Quorum	$0{,}05^{0,3}$	$1^{0,2}$	$0{,}6^{0,25}$	$0{,}6^{0,25}$
Corda	$1^{0,3}$	$1^{0,2}$	$0{,}6^{0,25}$	$0{,}4^{0,25}$
IOTA	$0{,}5^{0,3}$	$0{,}083^{0,2}$	$0{,}4^{0,25}$	$0{,}6^{0,25}$

Çizelge 2.39'da verilmiş olan üslere göre hesaplama yapılıp her bir satır değeri birbiri ile çarpıldıktan sonra Çizelge 2.40'ta verilmiş olan matris elde edilmektedir.

Çizelge 2.40. Her bir kritere göre alternatif değerlerinin ağırlıklara göre üsleri – AÇM

Kriter	**İşlem hacmi (saniyede işlem)**	**İşlem hızı (saniye)**	**Olgunluk düzeyi (1-5 aralığında)**	**Popülarite (1-5 aralığında)**	**Puan**
Ağırlık / Alternatif	**0,3**	**0,2**	**0,25**	**0,25**	
Ethereum	0,125892541	0,582	1,000	1,000	0,073245635
Hyperledger Fabric	0,592804395	1,000	0,880	0,946	0,493425652
Quorum	0,407090532	1,000	0,880	0,880	0,31533097
Corda	1	1,000	0,880	0,795	**0,699927102**
IOTA	0,812252396	0,608	0,795	0,880	0,345865754

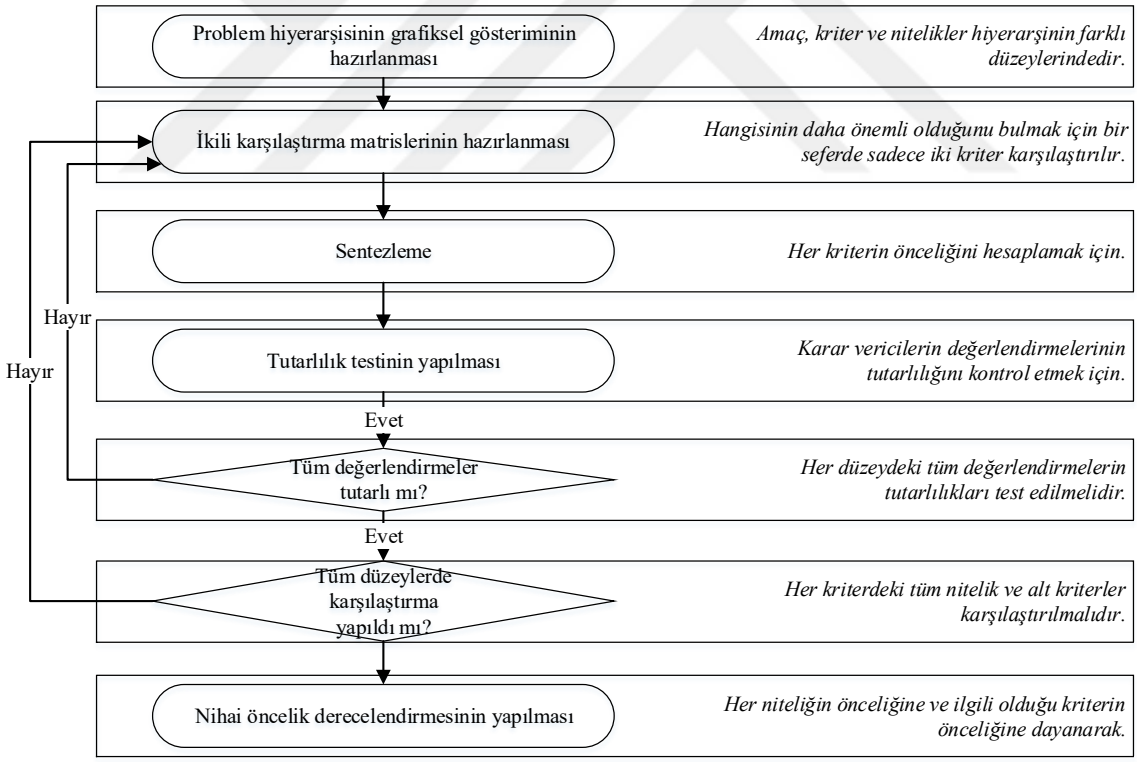
Puan değerleri hesaplandıktan sonra, aynı biçimde alternatifler yüksek puandan aşağı doğru sıralanır. Çizelge 2.40'ta verilmiş olan puanlara göre en iyi alternatif 0,699 puanla Corda'dır. Corda'yı sırasıyla Hyperledger Fabric, IOTA, Quorum ve Ethereum takip etmektedir.

2.7.3. Analitik Hiyerarşi Prosesi (The Analytic Hierarchy Process)

Thomas L. Saaty (1980) tarafından geliştirilmiş olan Analitik Hiyerarşi Prosesi (AHP) karmaşık konularda karar vermek için etkili bir araçtır ve karar vericiye öncelikleri belirlemek ve en iyi kararı vermek konusunda yardımcı olur. AHP karmaşık kararları ikişerli karşılaştırma dizilerine indirgeyip daha sonra sonuçları sentezleyerek karar için hem

sübjektif hem de objektif bir yaklaşım ortaya koyar, karar verme sürecindeki önyargıları elimine eder. AHP hem bireysel kararlarda hem de grup kararlarında kullanılabilir. Sadeliği, kullanım kolaylığı ve esnekliği nedeniyle AHP geliştirildiği tarihten bu yana Çok Kriterli Karar Verme ile ilgili hemen hemen tüm uygulamalarda yaygın biçimde kullanılmıştır.

AHP'nin üç temel unsuru hiyerarşinin oluşturulması, öncelik analizi ve tutarlılık doğrulamasıdır. İlk olarak, karar vericilerin karmaşık çok kriterli karar problemlerini, her olası özniteliğin birden çok hiyerarşik düzeyde düzenlendiği bileşen parçalarına ayırmaları gerekir. Daha sonra her parça, karar vericinin kendi yargısı doğrultusunda, aynı düzeyde ikili olarak birbirleriyle karşılaştırılır. Bu aşamadaki karşılaştırmalar kişisel ya da sübjektif olabileceğinden son aşamada bir tutarlılık doğrulaması yapılır ki bu doğrulama AHP'nin en önemli avantajıdır (Emrouznejad ve Ho, 2018: 1). (Ho, 2008)AHP adımlarını aşağıdaki akış şeması biçiminde ifade etmiştir:

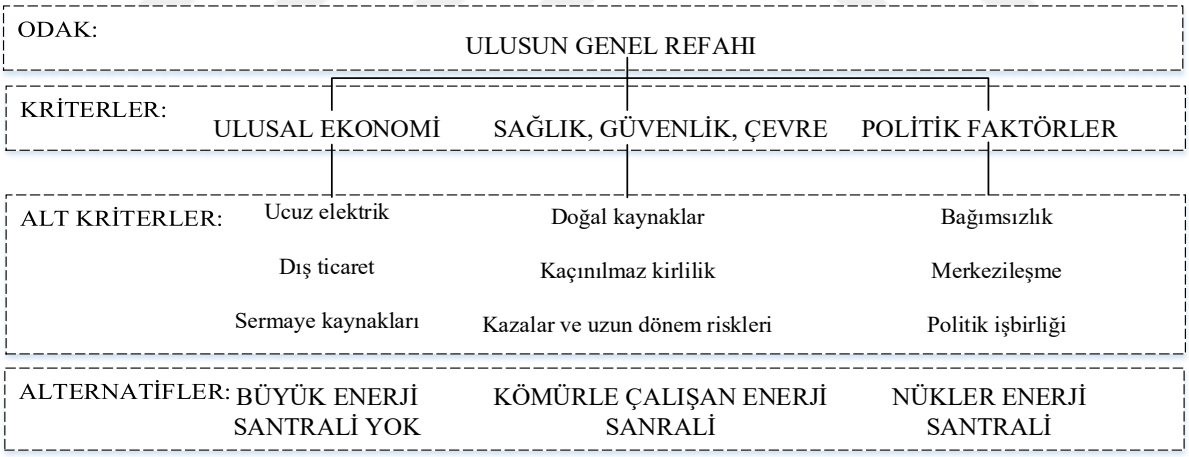


Şekil 2.15. AHP işlem adımları (Ho, 2008)

Uludağ ve Doğan'a (2016) göre AHP işlem kolaylığı ve anlaşılabilirlik avantajlarından dolayı Çok Kriterli Karar Vermede en sık tercih edilen yöntemlerden biri olup tek başına

kullanılabildiği gibi AHP ile kriter ağırlıkları belirlenip bu ağırlıklar başka yöntemlerde girdi olarak da kullanılabilmektedir.

AHP hem somut, ölçülebilir hem de soyut, ölçülemeyen alanlarda kullanılabilen bir metottur. AHP'nin bir problemi modellemede kullanılması için problemin hiyerarşik veya ağ yapısında ifade edilebilmesi ve bu yapı içerisinde ikili karşılaştırmalarla ilişkilerin kurulabilmesi gerekmektedir. AHP hem kesikli hem de sürekli ikişerli karşılaştırma durumlarında kullanılabilmekte olup kesikli durumlarda bu karşılaştırmalar baskınlık matrisleri olarak, sürekli durumlarda ise Fredholm operatörlerinin çekirdeği biçiminde kullanılır (Saaty R. W., 1987). AHP'de hiyerarşi en üst düzeyde verilmesi gereken karara ilişkin amacın (odak), ikinci düzeyde seçim için dikkate alınan ana kriterlerin, son düzeyde ise karar alternatiflerinin bulunduğu en az üç düzeyde oluşturulur. Ana kriterlerin altında gerekmesi halinde alt kriterlere de yer verilebilir. Bu yapıya ilişkin bir örnek olarak Hämäläinen ve Seppäläinen (1986) tarafından Finlandiya'da soyut kriterlere sahip büyük ölçekli bir sosyo-teknik problemin çözümü için geliştirilmiş olan AHP hiyerarşisi örneği Şekil 2.16'da verilmiştir.



Şekil 2.16. AHP hiyerarşik yapısına ilişkin "enerji santrali kararı" örneği (Hämäläinen ve Seppäläinen, 1986)

Gerçek hayat problemlerinin hiyerarşik yapısını oluşturmak kapsamlı bir çalışma gerektirmektedir. Bu hiyerarşik yapı ileriye ve geriye doğru olmak üzere iki tiptir. Hiyerarşik yapıdaki elemanlar kümeler halinde gruplandırılırlar. Bu homojen kümelerin düzeyi bir veya birden çok sayıda olabilir. Tamamlanmış bir hiyerarşik yapıda, bir düzeydeki tüm elemanlar kendinden sonra gelen tüm düzeyleri içerir (veri tabanındaki torun yapısı). Yukarıdaki

örnekte düzeyler kendi başlarına homojen kümeler biçiminde olup bu henüz tamamlanmamış bir hiyerarşik yapıdır (Saaty R. W., 1987).

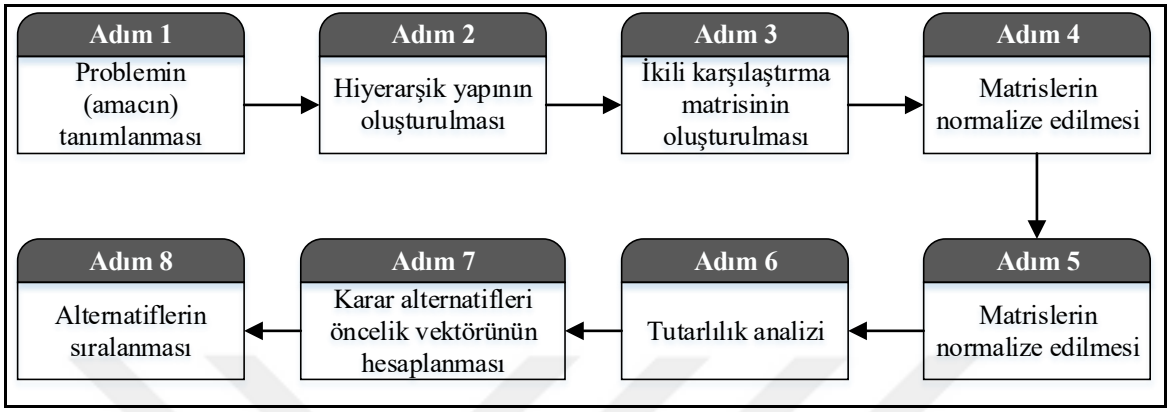
Hiyerarşik yapıda yer alacak düzey sayısı durumu ifade etmeye yeterli olacak kadar karmaşık ancak değişikliklere yeterli tepkiyi verebilecek kadar da basit olmalıdır. AHP'nin kullanımının temelinde ikili karşılaştırmalar yatmaktadır. Yukarıdaki örnekte, Finlandiya Parlamentosu öncelikle ana kriterler için önceliklerin göreceli önemlerine göre birbirleri ile ikili karşılaştırma yapıp ikili karşılaştırma matrisi oluşturmalıdır. Karşılaştırmaları yapmak için Çizelge 2.41'de verilmiş olan sayılarla ifade edilmiş temel ölçek kullanılır.

Çizelge 2.41. AHP için temel ölçek (Saaty R. W., 1987)

Mutlak ölçekte önem kuvveti	Tanım	Açıklama
1	Eşit önemde	İki faaliyet de hedefe eşit miktarda katkı sağlamaktadır
3	Biri diğerinden biraz daha (moderate) önemli (az üstünlük)	Deneyim ve yargılara göre bir faaliyet diğerine göre biraz daha önemlidir
5	Esaslı veya güçlü (essential or strong) önem	Deneyim ve yargılara göre bir faaliyet diğerine göre oldukça önemlidir
7	Çok güçlü önem (çok üstünlük)	Bir faaliyet çok kuvvetli biçimde önemlidir ve uygulamada baskınlığı gösterilmiştir
9	Son Derece Önemli (kesin üstünlük)	Bir faaliyetin diğerine göre önemi kanıtlarla en güçlü biçimde onaylanmaktadır
2, 4, 6, 8	Takip eden iki yargı arasındaki ara değerler (uzlaşı değerleri)	Farklı görüşler bulunması halinde uzlaşmaya gerek olduğunda kullanılır
Karşılıklı değerler (reciprocals)	Eğer *i* faaliyetine *j* ile karşılaştırılması sonucunda yukarıdaki değerlerden biri verilmişse, *j* bu durumda *i* ile karşılaştırıldığında karşılıklı değeri alacaktır.	Karşılıklı değer ile ifade edilmek istenen örneğin: *i*;*j* karşılaştırmasının önem kuvveti 3 ise bunun karşılığı olan *j*;*i* karşılaştırmasının değerinin 1/3 olmasıdır.
Oranlar (rationals)	Ölçekten elde edilen oranlar	Matrisi genişletmek için n adet sayısal değer elde edilerek tutarlılık zorlanacaksa

Karşılaştırılan unsur sayısı 'n' olmak üzere, 'n' sıralı bir matris için ikili karşılaştırmalardaki karar sayısı n(n-1)/2'dir (Çünkü; matrisin satır ve sütunları aynı unsurlardan oluştuğundan diyagonal unsurlar bire eşittir). Sonraki adımda her ana kritere ait alt kriterler karşılaştırılarak üç düzeyli hiyerarşik bir yapı için üç ikili karşılaştırma matrisi oluşturulur. Daha sonra üç alternatif her alt kritere göre karşılaştırılarak dördüncü düzey için dokuz ikili karşılaştırma matrisi oluşturulur. Son adım ise sonuçların bir araya getirilmesiyle nihai öncelikleri elde etmek için ağırlıklandırmanın yapılmasıdır (Saaty R. W., 1987).

Saaty R. W. (1987) AHP'nin ne olduğu ve nasıl kullanıldığını detaylı biçimde örneklendirerek açıklamış olup bu açıklamalar esas alınarak AHP metodu Şekil 2.17'de verildiği biçimde işlem adımlarına bölünmüş, her bir işlem adımı ayrıca detaylandırılmıştır.



Şekil 2.17. AHP işlem adımları

Adım 1. Üzerinde karar verilecek durumun ve amacın tanımlanması: Kriterler arasında karşılaştırma yapılırken sorulacak soru karşılaştırma değerlerini ve bunlara bağlı öncelikleri etkileyebilir. Bu nedenle, üzerinde karar verilecek durum ve bu duruma ilişkin amaç net biçimde tanımlanmalı, duruma ilişkin kriterlerin amacın yerine getirilmesine nasıl hizmet edeceği baştan açık biçimde belirlenmelidir. Sonraki adımlardaki işlemleri doğrudan etkilediğinden bu adımda yapılacak olan tanımlamalar çok önemlidir. Bu adımda karar problemi tanımlanarak amaç, uygun karar kriterleri yani karara etki eden unsurlar ve alternatifler tanımlanır. Bu tanımlama aşamasında sonraki adımda oluşturulacak olan hiyerarşik yapıya uygun biçimde veri toplanır.

Adım 2: Hiyerarşik yapının oluşturulması: Hiyerarşik yapı AHP'nin verilecek karara konu temel hedefi, karar verilecek konuya ilişkin kriter ve alt kriterler ile karar alternatifleri arasındaki ilişkiyi gösterir. Hiyerarşinin tepesinde ulaşılmak istenen temel amaç, en altında ise alternatifler yer alır. İkisinin arasında ise kriterler ve alt kriterler bulunur. Hiyerarşinin basamak sayısı ve karmaşıklığı standart olmayıp problemin yapısına bağlıdır.

Adım 3: İkili karşılaştırma matrislerinin oluşturulması: Bu aşamada, AHP temel ölçeği (Bkz. Çizelge 2.41) kullanılarak temel kriterler, alt kriterler ve karar alternatiflerinin ikili karşılaştırmaları yapılır. Bu ikili karşılaştırmalar satırları '*i*', sütunları '*j*' ile ifade edilmek

üzere köşegen elemanları 1 olan kare matris kullanılarak yapılır. Bu matrisin yapısı Eş. 2.3'te verilmiştir.

$$K=\begin{array}{c|ccccc} & Kr_1 & Kr_2 & Kr_3 & \dots & Kr_n \\ \hline Kr_1 & 1 & a_{12} & a_{13} & \dots & a_{1n} \\ Kr_2 & a_{21} & 1 & a_{23} & \dots & a_{2n} \\ Kr_3 & a_{31} & a_{32} & 1 & \dots & a_{3n} \\ . & . & . & . & \dots & . \\ . & . & . & . & \dots & . \\ . & . & . & . & \dots & . \\ Kr_n & a_{n1} & a_{n2} & a_{n3} & \dots & 1 \end{array} \quad (2.3)$$

Eş. 2.3'te verilmiş olan 'K' karşılaştırma matrisinde 'Kr' kriteri ifade etmek üzere, 'a_{ij}' *i*. kriter ile *j*. kriterin ikili karşılaştırma değeri olup *i*. kriterin *j*. kritere göre önem derecesini ifade etmektedir. Bu ikili karşılaştırma matrisinde a_{ji} değeri 1/ a_{ij}'ye eşittir ve buna karşılık olma özelliği denir.

Karşılaştırma matrisi oluşturularak ikili karşılaştırma yapılması tek seferlik bir işlem değildir. Bu aşamada, hem kriterler kendi içerisinde birbirleri ile ikişerli karşılaştırılır, hem de tüm alternatifler her bir kritere göre birbirleriyle karşılaştırılır. Örneğin; bir karar probleminde ölçeklenebilirlik, güvenlik ve merkezsizlik biçiminde üç kriter ve çözüm alternatifi olarak dört farklı blokzincir platformu varsa kriterler için 3x3, alternatifler için de 4x4 boyutunda bir karşılaştırma matrisi oluşturulur.

Adım 4: Matrislerin normalize edilmesi: Matrisin normalize edilmesi her elemanın kendi sütun toplamına bölünmesi ile gerçekleştirilir. Normalize edildikten sonra matrisin her sütununun toplamı 1'e eşit olur.

Adım 5: Öncelik vektörünün hesaplanması: Normalize edildikten sonra matrisin her bir satırının ortalaması bulunur. Hesaplanan bu satır ortalamaları o satırdaki kriterin önem derecesini, yani ağırlığını ifade eder. Her satırın ortalama değerinden oluşan 1x1 boyutlu matris öncelik vektörünü oluşturur ve bu vektör "W" ile ifade edilir.

Adım 6: Tutarlılık analizinin yapılması: Öncelik vektörü belirlendikten sonra karşılaştırma matrislerinin tutarlılığı hesaplanır. AHP'de tutarlılık hesaplaması için tutarlılık indeksi (CI;

Consistency Index) adlı katsayı kullanılır. CI katsayısının hesaplanması için kullanılan formül Eş. 2.4'te verilmiştir.

$$CI = \frac{\lambda_{max} - n}{n - 1} \tag{2.4}$$

Burada 'λ_{max}' maksimum özdeğeri (eigen vaue), 'n' ise kriter ya da alternatif sayısını ifade etmekte olup maksimum özdeğer Eş. 2.5 kullanılarak hesaplanır.

$$\lambda_{max} = \frac{1}{n}\sum_{i=1}^{n} \frac{\sum_{j=1}^{n} a_{ij} w_j}{w_i} \tag{2.5}$$

Eş. 2.5'te verilmiş olan formülün açılımı ise Eş. 2.6, 2.7 ve 2.8'de verilmiştir.

$$\text{K x W} = \begin{bmatrix} 1 & a_{12} & \cdots & a_{1n} \\ 1/a_{12} & 1 & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 1/a_{1n} & 1/a_{2n} & \cdots & 1 \end{bmatrix} \text{x} \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \tag{2.6}$$

$$d_i = \frac{x_i}{w_i}, i = 1,2, \dots, n \tag{2.7}$$

$$\lambda_{max} = \frac{\sum_{i=1}^{n} d_i}{n} \tag{2.8}$$

Tutarlılığın değerlendirilmesi için Rassal İndeks (RI – Random Index) değeri kullanılır. RI değeri hesaplanırken kullanılan simülasyon metodu ve hesaplama sürecinde üretilen matris sayısına bağlı olarak farklı araştırmacılar tarafından hesaplanan RI değerlerinde farklılıklar görülmektedir. Saaty (1980) 500 örneklem kullanarak n=10 için RI değerlerini Çizelge 2.42'de yer aldığı şekilde hesaplamıştır. Farklı yazarlarca hesaplanan RI değerleri aynı Çizelgede verilmiş olup bu çalışmada, hesaplama için kullanılan örneklem sayısının en fazla olduğu Alonso ve Lamata (2006) tarafından hesaplanmış olan RI değerleri kullanılmıştır. Aynı çalışmada, matrisin boyutu (karşılaştırılan kriter sayısı) arttıkça RI değerinin iyi biçimde tahmin edilmesinin güçleştiği belirtilmektedir.

Çizelge 2.42. Farklı yazarlar tarafından hesaplanmış RI değerleri (Alonso ve Lamata, 2006)

	RI (Rassal İndeks) değerleri				
Yazar	**Saaty (at Wharton)**	**Golden Wang**	**Noble**	**Aguaron vd.**	**Alonso & Lamata**
Örneklem n	500	1000	500	100 000	100 000
1	0	0	0	0	0
2	0	0	0	0	0
3	0,58	0,5799	0,49	0,525	0,5245
4	0,90	0,8921	0,82	0,882	0,8815
5	1,12	1,1159	1,03	1,115	1,1086
6	1,24	1,2358	1,16	1,252	1,2479
7	1,32	1,3322	1,25	1,341	1,3417
8	1,41	1,3952	1,31	1,404	1,4056
9	1,45	1,4537	1,36	1,452	1,4499
10	1,49	1,4882	1,39	1,484	1,4854
11	1,51	1,5117	1,42	1,513	1,5141
12		1,5356	1,44	1,535	1,5365
13		1,5571	1,46	1,555	1,5551
14		1,5714	1,48	1,570	1,5713
15		1,5831	1,49	1,583	1,5838

CI ve RI değerleri belirlendikten sonra Eş. 2.9 kullanılarak "Tutarlılık Oranı" (CR – Consistency Ratio) hesaplanır. Tutarlılık oranında tolerans %10'dur. Saaty (1980) tutarlılık oranının 0,10'u aşması durumunda problem üzerinde yeniden çalışılarak kriterlere ilişkin yargılarda değişiklik yapılmasını ve tutarlılık oranının belirtilen tolerans aralığına gelinceye dek bu biçimde kriter karşılaştırma yargılarının ayarlanmasını önermektedir. Tutarlılık oranı her bir kriter için ayrı ayrı hesaplanır.

$$CR = \frac{CI}{RI} \tag{2.9}$$

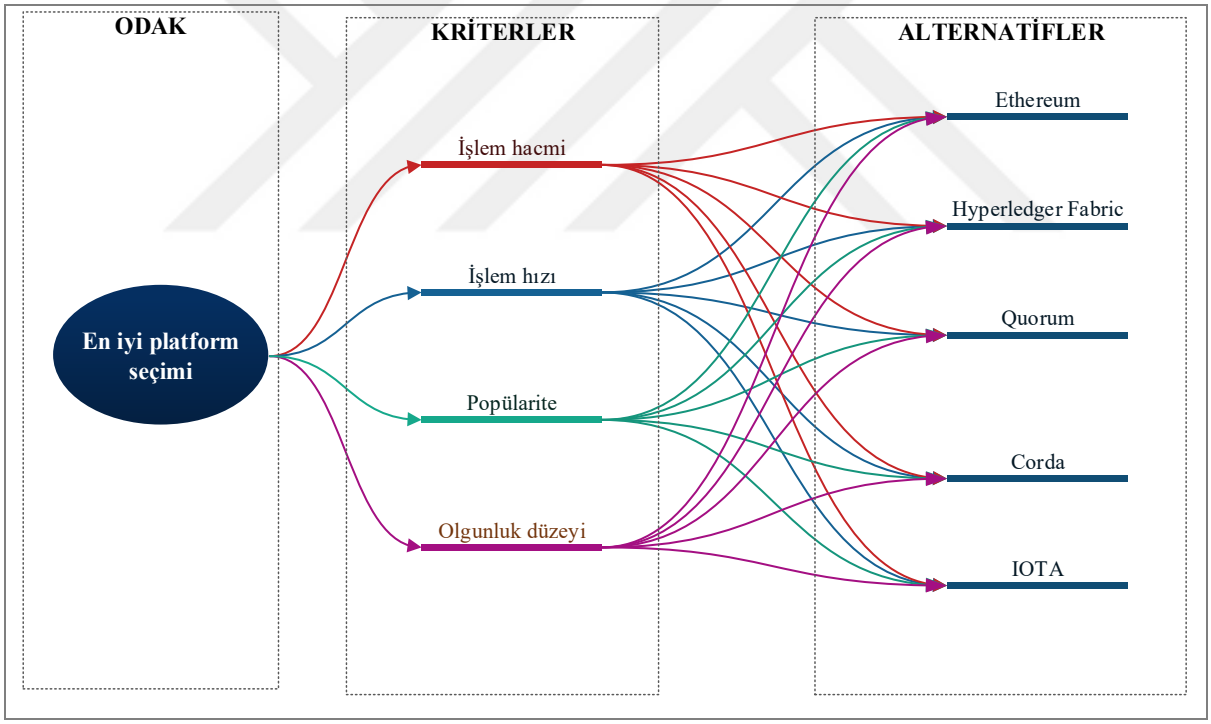
Adım 7: Karar alternatifleri öncelik vektörünün hesaplanması: Kriterler için ikili karşılaştırma matrisleri oluşturularak karar alternatifleri için öncelik vektörü hesaplanır. Öncelik vektörü hesaplanırken kriterlerin ikili karşılaştırma matrisi ile bulunan kriter ağırlıkları ile her bir alternatifin kriterlere göre karşılaştırmaları sonucunda bulunmuş olan kriterlere göre ağırlık matrisi birbiri ile çarpılır.

Adım 8: Karar alternatiflerinin ağırlıklarına göre sıralanması: Bu aşamada kriterler için elde edilen öncelik vektörleri birleştirilerek tüm öncelikler matrisi oluşturulur. Tüm öncelikler matrisi ile karar alternatiflerinin öncelik vektörü çarpılarak sonuç vektörü elde edilir. Bu

vektör karar alternatiflerinin ağırlıklarını verir. Bu ağırlıklar içerisinde en yüksek olan, tercih edilmesi gereken alternatifi ifade eder.

AHP hesaplamaları için örnek uygulama

Bu işlemlerin nasıl gerçekleştirildiği daha detaylı biçimde bir örnek üzerinden, blokzincir platformu seçim problemi ile gösterilmektedir. Bu örnekte, belirli bir kullanım senaryosu için AHP modeli kullanılarak platform seçimi yapılmaktadır. Örnek bir kullanım senaryosu için Ethereum, Hyperledger Fabric, Quorum, Corda ve IOTA platformları seçilmiş, bu platformları değerlendirmek için de işlem hacmi, işlem hızı, platformun olgunluk düzeyi ve popülaritesi olmak üzere dört kriter belirlenmiştir. Örnek için hiyerarşi modeli Şekil 2.18'de verilmiştir.



Şekil 2.18. Blokzincir platform seçimi için hiyerarşi modeli (AHP uygulama örneği)

Bu kriterlerin birbirlerine göre önem dereceleri için AHP temel ölçeği (Bkz. Çizelge 2.41) kullanılmaktadır. Buna göre;

- İşlem hacmi popülariteye ve olgunluğa göre çok güçlü önemde (7), işlem hızına göre biraz daha önemlidir (2).
- İşlem hızı olgunluğa ve popülariteye göre güçlü (5) önemdedir.

- Olgunluk ile popülarite eşit önemdedir (1).

Saaty'e göre (1987) hiyerarşik düzeylerine göre eleman çiftleri (i, j) bir ebeveyn unsura (odak veya hedef) göre birbirleriyle karşılaştırılarak önem dereceleri belirlenir. Bu önem dereceleri bir matris biçiminde oluşturulur. Matris karşılaştırma önem değerleri ile doldurulurken soldaki elemanlar (satır) 'i', üstteki elemanlar (sütun) 'j' olmak üzere, matrisin köşesinde yer alan kriter ya da hedef esas alınarak i ile j'den hangisinin kriteri daha fazla karşıladığı ya da o kritere göre daha önemli olduğu ve ne kadar daha önemli olduğu belirlenir. AHP temel ölçeğine göre belirlenen önem derecesi 'a_{ij}' (veya a_{ji}) değerini verir. Matristeki bu hücrenin değerinin karşılığı ise otomatik olarak transpoz için girilir. Blokzincir platformu seçimine ilişkin örnekteki ana hedefe göre belirlenmiş olan kriterlerin ikili karşılaştırmasını içeren matris Çizelge 2.43'te verilmiştir.

Çizelge 2.43. Blokzincir platform seçim kriterleri ikili karşılaştırma matrisi (AHP uygulama örneği)

Hedef/Odak	**İşlem hacmi**	**İşlem hızı**	**Olgunluk**	**Popülarite**
İşlem hacmi	1	2	7	7
İşlem hızı	1/2	1	5	5
Olgunluk	1/7	1/5	1	1
Popülarite	1/7	1/5	1	1
Toplam	1,786	3,400	14,000	14,000

Çizelge 2.43'te verilmiş olan matriste dikkat edilmesi gereken ilk karşılaştırma (işlem hızı, işlem hacmi) karşılaştırmasıdır. İşlem hacmi işlem hızına göre biraz daha önemli olup (2) bu durumda karşılık değeri (2,1) pozisyonuna 1/2 olarak girilmiştir. Otomatik olarak, bu hücrenin transpozu olan (1, 2) hücresinin değeri (işlem hacmi, işlem hızı) için 2 değerini almaktadır. Bu biçimde, diğer karşılaştırma değerleri de belirlenerek ilk matris oluşturulmuştur.

Sonraki adımda, ilk oluşturulan ikili karşılaştırma matrisi (Çizelge 2.43) normalize edilir. Bu işlem için, her bir hücre değeri ilgili sütunun toplam değerine bölünür. Böylece her bir sütundaki öncelik değelerinin toplamı bire eşit olur. Normalize edilmiş ikili karşılaştırma matrisi Çizelge 2.44'te verilmiştir. Normalize edilmiş matris üzerinde ayrıca her bir satırın ortalama değeri alınarak hesaplanan ağırlık değerleri de verilmiştir.

Çizelge 2.44. Normalize edilmiş ikili karşılaştırma matrisi (AHP uygulama örneği)

Hedef/Odak	İşlem hacmi	İşlem hızı	Olgunluk	Popülarite	Ağırlık
İşlem hacmi	0,560	0,588	0,500	0,500	0,537
İşlem hızı	0,280	0,294	0,357	0,357	0,322
Olgunluk	0,080	0,059	0,071	0,071	0,070
Popülarite	0,080	0,059	0,071	0,071	0,070

Bu adımda hesaplanan ağırlık değerlerine göre oluşan öncelik vektörü sırasıyla işlem hacmi, işlem hızı, olgunluk ve popülarite için [0,537; 0,322; 0,070; 0,070] biçimindedir.

Bir sonraki adımda öncelik vektörü için tutarlılık analizi yapılır. Bir matrisin tutarlı olması için her i, j ve k değeri için $a_{ij}.a_{jk}=a_{ik}$ eşitliği sağlanmalıdır. Verilen örnekteki matris (Bkz. Çizelge 2.43) bu şartı sağlamadığından tutarsız olarak nitelendirilmektedir. Örneğin, matrise göre (İşlem hacmi, İşlem hızı) = 2 iken (İşlem hızı, Olgunluk) = 5 olduğundan matrisin tutarlı olması için (İşlem hacmi, Olgunluk) = (İşlem hacmi, İşlem hızı) x (İşlem hızı, Olgunluk) eşitliği sağlanmalıdır. Ancak, örnek matriste (İşlem hacmi, Olgunluk) değeri 7, eşitliğin sağ tarafındaki çarpım değeri ise (2 x 5) = 10'dur. Matristeki (İşlem hacmi, Olgunluk) karşılaştırmasına denk gelen (1, 3) pozisyonunun değeri olan 7, tutarlılık için gerekli olan 10 değerinden küçüktür. Bu değerin karşılık değeri ise (3, 1) pozisyonundaki 1/7 olup bu değer de tutarlılık için gerekli olan 10'un karşılığı olan 1/10'dan büyüktür. Yani, bir değer ilgili tutarlılık değerini aşarken bunun karşılığı olan değer ise tutarlılık değerinin altında kalmaktadır. Bunun anlamı, matris içerisinde tutarsızlığı telafi etme eğiliminin olmasıdır. 'n' boyutlu pozitif karşılıklı (reciprocal) bir matris tutarlı olduğunda ana özdeğer (principal eigenvalue) 'n' değerini alır. Tutarsız olduğunda ise özdeğer n'i aşar ve bu aşım değeri tutarsızlığın derecesini gösterir. Tutarlılık Oranı (Consistency Ratio – CR) olarak ifade edilen bu derece kullanılarak karşılaştırma matrisinin tutarlılığı hesaplanır. Örnek için ilgili tutarlılık analizi formülleri (Bkz. Eş. 2.6, 2.7 ve 2.8) kullanılarak yapılan hesaplama sonucunda elde edilen matris Çizelge 2.45'te verilmiştir.

Çizelge 2.45. Platform özellikleri için tutarlılık analizi değerleri (AHP uygulama örneği)

Hedef/Odak	İşlem hacmi	İşlem hızı	Olgunluk	Popülarite	Toplam	Ağırlık	Toplam/ Ağırlık
İşlem hacmi	0,537	0,644	0,493	0,493	2,167	0,537	4,035206
İşlem hızı	0,269	0,322	0,352	0,352	1,295	0,322	4,019958
Olgunluk	0,077	0,064	0,070	0,070	0,282	0,070	4,004296
Popülarite	0,077	0,064	0,070	0,070	0,282	0,070	4,004296
						Ortalama (λ_{max})	4,015939

Çizelge 2.45'te 'Toplam/Ağırlık' sütununun ortalaması λ_{max} değerini vermektedir. Buna göre;

$CI = \frac{\lambda_{max}-n}{n-1} = \frac{4,016-4}{3} = 0,005$ bulunur. Daha sonra Çizelge 2.42'de yer alan Rassal İndeks değerlerinden n=4'e karşılık gelen değer bulunarak Tutarlılık Oranı (CR) hesaplanır. Kriter sayısı dört olduğundan RI değeri 0,88'tir. Buna göre;

$CR = \frac{CI}{RI} = \frac{0,05}{0,88} \approx 0,06$ bulunur. Bu değer limit değer olan 0,10'dan küçük olduğu için karşılaştırma matrisi tutarlıdır ve sonraki işlem adımlarına devam edilebilir. Sonraki adımda her bir alternatifin her bir kritere göre ayrı ayrı ikili karşılaştırması yapılır. Örnek için ikili karşılaştırmalar yapılırken blokzincir platformlarının kriter özellikleri (Bkz. Çizelge 2.35) kullanılmış, bu özellikler AHP temel ölçeği (Bkz. Çizelge 2.41) kullanılarak değerlendirilmiş ve kriterlere göre karşılaştırma matrisleri oluşturulmuştur. Buna göre, bu özellikler aşağıda listelenmiştir:

- İşlem hacmi
  - İşlem hacmi en yüksek olan Corda (saniyede 20 000) Ethereum'a (saniyede 20) son derece üstün (9), Hyperledger Fabric'e (saniyede 3 500) göre güçlü önemde (5), Quorum'a (saniyede 1 000) göre çok güçlü önemde (7), IOTA'ya (saniyede 10 000) göre ise biraz daha önemlidir (3).
  - IOTA Ethereum'a göre çok güçlü ile son derece önemli arasında (8) önemde, Hyperledger Fabric'e göre biraz daha önemli (4), Quorum'a göre güçlü önemdedir (5).
  - Hyperledger Fabric Ethereum'a göre çok güçlü önemde (6), Quorum'a göre güçlü önemdedir (3).
  - Quorum Ethereum'a göre güçlü önemdedir (5).

Bu verilenlere göre oluşturulan ilk karşılaştırma matrisi Çizelge 2.46'da verilmiştir.

Çizelge 2.46. İşlem hacmi kriterine göre platform alternatiflerinin ikili karşılaştırma matrisi

İŞLEM HACMİ	**Ethereum**	**Hyp. Fab.**	**Quorum**	**Corda**	**IOTA**
Ethereum	1	1/6	1/5	1/9	1/8
Hyp. Fab.	6	1	3	1/5	1/4
Quorum	5	1/3	1	1/7	1/5
Corda	9	5	7	1	3
IOTA	8	4	5	1/3	1
Toplam	29,0000	8,5000	16,2000	1,7873	4,8250

Platform alternatiflerinin ikili karşılaştırma matrisi normalize edildikten sonra oluşan matris Çizelge 2.47'de verilmiştir:

Çizelge 2.47. Normalize edilmiş ikili karşılaştırma matrisi – İşlem Hacmi (AHP uygulama örneği)

İŞLEM HACMİ	Ethereum	Hyp. Fab.	Quorum	Corda	IOTA	Ağırlık (w)
Ethereum	0,0345	0,0159	0,0123	0,0622	0,0273	0,0304
Hyp. Fab.	0,2069	0,0952	0,1852	0,1119	0,0546	0,1308
Quorum	0,1724	0,0317	0,0617	0,0799	0,0437	0,0779
Corda	0,3103	0,4762	0,4321	0,5595	0,6557	0,4868
IOTA	0,2759	0,3810	0,3086	0,1865	0,2186	0,2741
Toplam	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000

Çizelge 2.47'de verilmiş olan normalize edilmiş matrise göre platform alternatiflerinin öncelik matrisi [Ethereum; Hyperledger Fabric; Quorum; Corda; IOTA] = [0,0304; 0,1308; 0,0779; 0,4868; 0,2741] biçimindedir.

İşlem hacmine göre ikili karşılaştırma matrisindeki değerler ile bu öncelik matrisinden, Çizelge 2.48'de verilmiş olan eşitliklere göre yapılacak hesaplamalarda faydalanılmaktadır.

Çizelge 2.48. Tutarlılık analizi hesaplamalarında kullanılan hesaplama ve formüller (AHP uygulama örneği)

İŞLEM HACMİ	Ethereum	Hyp. Fab.	Quorum	Corda	IOTA	Ağırlık (w)
Ethereum	$a_{11}xw_1$	$a_{12}\ xw_2$	$a_{13}\ xw_3$	$a_{14}\ xw_4$	$a_{15}\ xw_5$	w_1
Hyp. Fab.	$a_{21}xw_1$	$a_{22}\ xw_2$	$a_{23}\ xw_3$	$a_{24}\ xw_4$	$a_{25}\ xw_5$	w_2
Quorum	$a_{31}\ xw_1$	$a_{32}\ xw_2$	$a_{33}\ xw_3$	$a_{34}\ xw_4$	$a_{35}\ xw_5$	w_3
Corda	$a_{41}\ xw_1$	$a_{42}\ xw_2$	$a_{43}\ xw_3$	$a_{44}\ xw_4$	$a_{45}\ xw_5$	w_4
IOTA	$a_{51}\ xw_1$	$a_{52}\ xw_2$	$a_{53}\ xw_3$	$a_{54}\ xw_4$	$a_{55}\ xw_5$	w_5
Eşitlikler	$CI = \frac{\lambda_{max}-n}{n-1}$; $\lambda_{max} = \frac{1}{n}\sum_{i=1}^{n}\frac{\sum_{j=1}^{n} a_{ij}w_j}{w_i}$					

Çizelge 2.48'de verilmiş olanlar kullanılarak yapılan hesaplamalar sonucunda elde edilen sonuçlar Çizelge 2.49'da verilmiştir.

Çizelge 2.49. İşlem hacmine göre platform alternatifleri için tutarlılık analizi hesaplamaları (AHP uygulama örneği)

İŞLEM HACMİ	Eth.	Hyp. Fab.	Quo.	Corda	IOTA	Topl.	Ağırlık	T/A
Ethereum	0,0304	0,0218	0,0156	0,0541	0,0343	0,1562	0,0304	5,131

İŞLEM HACMİ	Eth.	Hyp. Fab.	Quo.	Corda	IOTA	Topl.	Ağırlık	T/A
Hyp. Fab.	0,1826	0,1308	0,2337	0,0974	0,0685	0,7130	0,1308	5,452
Quorum	0,1522	0,0436	0,0779	0,0695	0,0548	0,3980	0,0779	5,109
Corda	0,2739	0,6539	0,5453	0,4868	0,8223	2,7823	0,4868	5,716
IOTA	0,2435	0,5231	0,3895	0,1623	0,2741	1,5925	0,2741	5,810
Ortalama (λ_{max})								5,444
CI ($\frac{\lambda_{max}-n}{n-1}$)								0,111
RI (Bkz. Çizelge 2.42)								1,11
$CR = \frac{CI}{RI}$								0,09988

Çizelge 2.49'da verilmiş olan hesaplamalarda da görüleceği üzere Tutarlılık Oranı (CR) eşik değeri olan 0,10'dan küçük olduğundan karşılaştırma matrisi tutarlıdır ve sonraki işlem adımlarına devam edilebilir. Bir sonraki işlem adımında aynı biçimde, işlem hızı kriteri için hesaplamalar gerçekleştirilmektedir.

- İşlem hızı
  - İşlem hızı kriteri 'maliyet' kriteri olarak değerlendirilmekte olup diğer kriterlerin aksine, düşük değerli olması istenen durumdur.
  - İşlem hızı en yüksek olan (1 saniye) Hyperledger Fabric, Quorum ve Corda birbirleri ile eşit önemdedir (1).
  - Hyperledger Fabric, Quorum ve Corda işlem hızı 12 sn olan IOTA'ya göre biraz daha önemli (3), işlem hızı 15 sn olan Ethereum'a göre ise daha önemlidir (4).
  - İşlem hızı 12 sn olan IOTA Ethereum'dan biraz daha üstündür (2).

Bu verilenlere göre oluşturulan ilk karşılaştırma matrisi Çizelge 2.50'de verilmiştir.

Çizelge 2.50. İşlem hızı kriterine göre platform alternatiflerinin ikili karşılaştırma matrisi (AHP uygulama örneği)

İŞLEM HIZI	Ethereum	Hyp. Fab.	Quorum	Corda	IOTA
Ethereum	1	1/4	1/4	1/4	1/2
Hyp. Fab.	4	1	1	1	3
Quorum	4	1	1	1	3
Corda	4	1	1	1	3
IOTA	2	1/3	1/3	1/3	1
Toplam	15,0000	3,5833	3,5833	3,5833	10,5000

Bu adımdan sonra oluşturulan normalizasyon matrisi Çizelge 2.51'de verilmiştir.

Çizelge 2.51. Normalize edilmiş ikili karşılaştırma matrisi – İşlem Hızı (AHP uygulama örneği)

İŞLEM HIZI	Ethereum	Hyp. Fab.	Quorum	Corda	IOTA	Ağırlık
Ethereum	0,0667	0,0698	0,0698	0,0698	0,0476	0,0647
Hyp. Fab.	0,2667	0,2791	0,2791	0,2791	0,2857	0,2779
Quorum	0,2667	0,2791	0,2791	0,2791	0,2857	0,2779
Corda	0,2667	0,2791	0,2791	0,2791	0,2857	0,2779
IOTA	0,1333	0,0930	0,0930	0,0930	0,0952	0,1015
Toplam	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000

Sonraki adımda gerçekleştirilen tutarlılık analizi hesaplamaları Çizelge 2.52'de verilmiştir.

Çizelge 2.52. İşlem hızına göre platform alternatifleri için tutarlılık analizi hesaplamaları (AHP uygulama örneği)

İŞLEM HIZI	Eth.	Hyp. Fab.	Quo.	Corda	IOTA	Topl.	Ağırlık	T/A
Ethereum	0,0647	0,0695	0,0695	0,0695	0,0508	0,3239	0,0647	5,005
Hyp. Fab.	0,2589	0,2779	0,2779	0,2779	0,3046	1,3972	0,2779	5,027
Quorum	0,2589	0,2779	0,2779	0,2779	0,3046	1,3972	0,2779	5,027
Corda	0,2589	0,2779	0,2779	0,2779	0,3046	1,3972	0,2779	5,027
IOTA	0,1294	0,0926	0,0926	0,0926	0,1015	0,5089	0,1015	5,012
Ortalama (λ_{max})								5,020
CI ($\frac{\lambda_{max}-n}{n-1}$)								0,005
RI (Bkz. Çizelge 2.42)								1,11
$CR = \frac{CI}{RI}$								0,004486

Çizelge 2.52'de verilmiş olan hesaplamalarda da görüleceği üzere Tutarlılık Oranı (CR) eşik değeri olan 0,10'dan küçük olduğundan karşılaştırma matrisi tutarlıdır ve sonraki işlem adımlarına devam edilebilir. Bir sonraki işlem adımında aynı biçimde, olgunluk düzeyi kriteri için hesaplamalar gerçekleştirilmektedir.

- Olgunluk düzeyi
  - Hyperledger Fabric, Quorum ve Corda '3' olan olgunluk düzeyleri ile, birbirleri ile eşit önemdedir (1).
  - Olgunluk düzeyi en yüksek (5) olan Ethereum Hyperledger Fabric, Quorum ve Corda'ya göre biraz daha önemli (3), IOTA'ya göre güçlü önemdedir (5).

- Hyperledger Fabric, Quorum ve Corda IOTA'ya göre biraz önemlidir (2).

Bu verilenlere göre oluşturulan ilk karşılaştırma matrisi Çizelge 2.53'te verilmiştir.

Çizelge 2.53. Olgunluk kriterine göre platform alternatiflerinin ikili karşılaştırma matrisi (AHP uygulama örneği)

OLGUNLUK	**Ethereum**	**Hyp. Fab.**	**Quorum**	**Corda**	**IOTA**
Ethereum	1	3	3	3	5
Hyp. Fab.	1/3	1	1	1	2
Quorum	1/3	1	1	1	2
Corda	1/3	1	1	1	2
IOTA	1/5	1/2	1/2	1/2	1
Toplam	2,2000	6,5000	6,5000	6,5000	12,0000

Bu adımdan sonra oluşturulan normalizasyon matrisi Çizelge 2.54'te, sonraki adımda gerçekleştirilen tutarlılık analizi hesaplamaları ise Çizelge 2.55'te verilmiştir.

Çizelge 2.54. Normalize edilmiş ikili karşılaştırma matrisi – Olgunluk (AHP uygulama örneği)

OLGUNLUK	**Ethereum**	**Hyp. Fab.**	**Quorum**	**Corda**	**IOTA**	**Ağırlık**
Ethereum	0,4545	0,4615	0,4615	0,4615	0,4167	0,4512
Hyp. Fab.	0,1515	0,1538	0,1538	0,1538	0,1667	0,1559
Quorum	0,1515	0,1538	0,1538	0,1538	0,1667	0,1559
Corda	0,1515	0,1538	0,1538	0,1538	0,1667	0,1559
IOTA	0,0909	0,0769	0,0769	0,0769	0,0833	0,0810
Toplam	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000

Çizelge 2.55. Olgunluğa göre platform alternatifleri için tutarlılık analizi hesaplamaları (AHP uygulama örneği)

OLGUNLUK	**Eth.**	**Hyp. Fab.**	**Quo.**	**Corda**	**IOTA**	**Topl.**	**Ağırlık**	**T/A**
Ethereum	0,4512	0,4678	0,4678	0,4678	0,4050	2,2597	0,4512	5,009
Hyp. Fab.	0,1504	0,1559	0,1559	0,1559	0,1620	0,7802	0,1559	5,003
Quorum	0,1504	0,1559	0,1559	0,1559	0,1620	0,7802	0,1559	5,003
Corda	0,1504	0,1559	0,1559	0,1559	0,1620	0,7802	0,1559	5,003
IOTA	0,0902	0,0780	0,0780	0,0780	0,0810	0,4052	0,0810	5,002
Ortalama (λ_{max})								5,004
CI ($\frac{\lambda_{max}-n}{n-1}$)								0,001
RI (Bkz. Çizelge 2.42)								1,11
$CR = \frac{CI}{RI}$								0,000899

Çizelge 2.55'te verilmiş olan hesaplamalarda da görüleceği üzere Tutarlılık Oranı (CR) eşik değeri olan 0,10'dan küçük olduğundan karşılaştırma matrisi tutarlıdır ve sonraki işlem adımlarına devam edilebilir. Bir sonraki işlem adımında aynı biçimde, popülarite kriteri için hesaplamalar gerçekleştirilmektedir.

- Popülarite
  - Popülarite puanı en yüksek (5) olan Ethereum Hyperledger Fabric'den biraz daha önemli (3), Quorum ve IOTA'ya göre güçlü önemde (5), Corda'ya göre ise çok güçlü önemdedir (7).
  - Popülarite puanı 4 olan Hyperledger Fabric Quorum ve IOTA'ya göre biraz daha güçlü önemde (3), Corda'ya göre ise güçlü öndemdedir (5).
  - Quourum ile IOTA birbirlerine göre eşit önemde, Corda'ya göre ise biraz daha önemlidir (3).

Bu verilenlere göre oluşturulan ilk karşılaştırma matrisi Çizelge 2.56'da, daha sonra oluşturulan normalizasyon matrisi ise Çizelge 2.57'de verilmiştir.

Çizelge 2.56. Popülarite kriterine göre platform alternatiflerinin ikili karşılaştırma matrisi (AHP uygulama örneği)

POPÜLARİTE	**Ethereum**	**Hyp. Fab.**	**Quorum**	**Corda**	**IOTA**
Ethereum	1	3	5	7	5
Hyp. Fab.	1/3	1	3	5	3
Quorum	1/5	1/3	1	3	1
Corda	1/7	1/5	1/3	1	1/3
IOTA	1/5	1/3	1	3	1
Toplam	1,8762	4,8667	10,3333	19,0000	10,3333

Çizelge 2.57. Normalize edilmiş ikili karşılaştırma matrisi – Popülarite (AHP uygulama örneği)

POPÜLARİTE	**Ethereum**	**Hyp. Fab.**	**Quorum**	**Corda**	**IOTA**	**Ağırlık**
Ethereum	0,5330	0,6164	0,4839	0,3684	0,4839	0,4971
Hyp. Fab.	0,1777	0,2055	0,2903	0,2632	0,2903	0,2454
Quorum	0,1066	0,0685	0,0968	0,1579	0,0968	0,1053
Corda	0,0761	0,0411	0,0323	0,0526	0,0323	0,0469
IOTA	0,1066	0,0685	0,0968	0,1579	0,0968	0,1053
Toplam	1,0000	1,0000	1,0000	1,0000	1,0000	1,0000

Sonraki adımda gerçekleştirilen tutarlılık analizi hesaplamaları Çizelge 2.58'de verilmiştir.

Çizelge 2.58. Popülariteye göre platform alternatifleri için tutarlılık analizi hesaplamaları (AHP uygulama örneği)

POPÜLARİTE	**Eth.**	**Hyp. Fab.**	**Quo.**	**Corda**	**IOTA**	**Topl.**	**Ağırlık**	**T/A**
Ethereum	0,4971	0,7362	0,5265	0,3281	0,5265	2,6145	0,4971	5,259
Hyp. Fab.	0,1657	0,2454	0,3159	0,2344	0,3159	1,2773	0,2454	5,205
Quorum	0,0994	0,0818	0,1053	0,1406	0,1053	0,5325	0,1053	5,056
Corda	0,0710	0,0491	0,0351	0,0469	0,0351	0,2372	0,0469	5,060
IOTA	0,0994	0,0818	0,1053	0,1406	0,1053	0,5325	0,1053	5,056
Ortalama (λ_{max})								5,127
CI ($\frac{\lambda_{max}-n}{n-1}$)								0,032
RI (Bkz. Çizelge 2.42)								1,11
$CR = \frac{CI}{RI}$								0,028683

Çizelge 2.58'de verilmiş olan hesaplamalarda da görüleceği üzere Tutarlılık Oranı (CR) eşik değeri olan 0,10'dan küçük olduğundan karşılaştırma matrisi tutarlıdır ve sonraki işlem adımlarına devam edilebilir.

Bir sonraki adımda tüm kriterlere göre alternatiflerin ikili karşılaştırmaları sonucunda elde edilen ağırlık vektörleri kullanılarak alternatif-kriter matrisi oluşturulmaktadır. Örnek için oluştururan matris Çizelge 2.59'da verilmiştir.

Çizelge 2.59. Alternatiflerin ikili karşılaştırmaları sonucunda elde edilen ağırlık vektörleri (AHP uygulama örneği)

Kriter / **Alternatif**	**İşlem hacmi**	**İşlem hızı**	**Olgunluk**	**Popülarite**
Ethereum	0,0304	0,0647	0,4512	0,4971
Hyp. Fab.	0,1308	0,2779	0,1559	0,2454
Quorum	0,0779	0,2779	0,1559	0,1053
Corda	0,4868	0,2779	0,1559	0,0469
IOTA	0,2741	0,1015	0,0810	0,1053

Tutarlılık oranının (CR) 0,10'i aşması halinde ikili karşılaştırmalarda verilen öncelik değerlerinin yeniden değerlendirilerek düzenlenmesi gerekmektedir. Tüm karşılaştırma matrisleri için CR'nin eşik değerinin altında olması sağlandıktan sonra nihai alternatif

önceliklendirme hesabı için Çizelge 2.59'daki alternatiflerin kriterlere göre ağırlıklarının matrisi ile seçim kriterlerinin ikili karşılaştırma matrisinden (Bkz. Çizelge 2.44) elde edilen ağırlık vektörü (tablonun son sütunu) çarpılır. Bu çarpım işlemi Eş. 2.10'da verilmiştir.

$$\begin{vmatrix} 0{,}0304 & 0{,}0647 & 0{,}4512 & 0{,}4971 \\ 0{,}1308 & 0{,}2779 & 0{,}1559 & 0{,}2454 \\ 0{,}0779 & 0{,}2779 & 0{,}1559 & 0{,}1053 \\ 0{,}4868 & 0{,}2779 & 0{,}1559 & 0{,}0469 \\ 0{,}2741 & 0{,}1015 & 0{,}0810 & 0{,}1053 \end{vmatrix} \text{X} \begin{vmatrix} 0{,}537 \\ 0{,}322 \\ 0{,}07 \\ 0{,}07 \end{vmatrix} = \begin{vmatrix} \mathbf{0{,}1035392} & \text{Ethereum (5)} \\ \mathbf{0{,}1878144} & \text{Hyp. Fab. (3)} \\ \mathbf{0{,}1496001} & \text{Quorum (4)} \\ \mathbf{0{,}3650914} & \text{Corda (1)} \\ \mathbf{0{,}1929157} & \text{IOTA (2)} \end{vmatrix} \quad (2.10)$$

Bu çarpım sonucunda elde edilen vektör (Eş. 2.10'da koyu renkte gösterilmiştir), her bir karar alternatifinin seçim için kullanılacak ağırlığını verir. Bu sonuca göre öncelik değeri 0,365 ile en yüksek olan Corda seçim için ilk sırada gelmelidir. İkinci sıradaki seçim ise 0,1929 değeri ile IOTA'dır. Tüm alternatiflerin öncelik sıralaması Eş. 2.10'da son sütunda parantez içerisinde verilmiştir.

2.7.4. Revize Edilmiş Analitik Hiyerarşi Prosesi (The Revised Analytic Hierarchy Process)

Belton ve Gear (1983) tarafından öne sürülen Revize Edilmiş AHP orijinal AHP'nin bir çeşididir. Belton ve Gear çalışmalarında, mevcut alternatiflerden birine benzer bir alternatifin eklendiğinde AHP'nin alternatiflerin sıralamasını tersine çevirebileceğini gözlemlemiş, bu eksikliği gidermek için AHP karar matrisinin her bir sütununun o sütunun maksimum değerine bölünmesini önermiştir.

Dyer (1990) çalışmasında hiçbir özdeş alternatif bulunmasa bile AHP'nin keyfi sıralamalarla sonuçlanabileceğini göstermiştir. Dyer AHP'nin bazı durumlarda tutarlı bir karar vericinin gerçek performansına yakın sonuçlar verebileceğini ve alternatiflerin doğru biçimde sıralanabileceğini kabul etmekle birlikte genel olarak bunun olmayacağını öne sürmektedir.

Triantaphyllou ve Mann (1994) karar verme problemlerinde Saaty ikili karşılaştırma matrislerinin girdi olarak kullanıldığında ortaya çıkan alternatif sıralamasındaki ters çevrilmeleri araştırmıştır. Bu ikili karşılaştırma matrisleri gerçek dünyadaki birçok karar verme durumunda başarıyla kullanılmaktadır. Bu çalışmada, AHP ve Revize edilmiş AHP yöntemlerinin alternatiflerin sıralanmasında ciddi başarısızlıkla sonuçlanabileceği ortaya

konularak başarısızlıkların alternatif sayısı arttıkça arttığı ileri sürülmektedir. Kriter sayısının bu başarısızlık oranına etkisi oldukça düşük olup alternatif sayısı beşin üzerine çıktığında hata oranı %50'yi aşmaktadır.

2.7.5. Bulanık Analitik Hiyerarşi Prosesi (The Fuzzy Analytic Hierarchy Process)

Bulanık mantık kavramı ilk olarak 1965 yılında, Lukasiewicz'in üç değerli mantık sistemini kullanarak küme teorisini geliştiren ve geliştirdiği bu kümeyi bulanık küme olarak adlandıran Lotfi A. Zadeh tarafından ortaya atılmıştır. Bu yeni küme yapısında küme elemanları klasik mantıktaki gibi bir kümenin elemanı olmak (1) ya da elemanı olmamak (0) durumu dışında, farklı derecelerde aitlik değeri taşımaktadır.

Klasik küme teorisinde bir eleman kümeye ya aittir ya da değildir. Buna karşılık, bulanık küme teorisi, bir kümedeki elemanların üyeliğinin kademeli olarak değerlendirilmesine izin verir. Bu kademeli değerlendirme [0, 1] gerçek birim aralığında değer verilen bir üyelik fonksiyonu yardımıyla açıklanır (Dubois, Lang ve Prade, 1991).

AHP her ne kadar nitel verileri içeren çok kriterli analiz problemlerini çözmek için popüler bir yöntem olsa da kullandığı dengesiz kişisel yargılar ve ikili karşılaştırma sürecinin doğasında bulunan belirsizliği ele alma konusundaki yetersizliği nedeniyle eleştirilmektedir (Deng, 1999). AHP'nin belirsizlik ve sübjektifliğine dayalı bu kısıtlılıklarını gidermek için insan düşünce yapısına daha yakın bir yöntem olan bulanık mantık kullanılarak AHP geliştirilmiş, bu biçimde Bulanık AHP yöntemi ortaya konmuştur.

Bulanık mantığın işleyişine benzer biçimde, bulanık AHP'de karar verici değerlendirmelerinin linguistik ifadeleri bulanık sayılara dönüştürülerek AHP ile aynı adımlar izlenir. Bulanık AHP'de önem tablosu üçgen bulanık sayılar kullanılması halinde Çizelge 2.60'ta verildiği biçimdedir:

Çizelge 2.60. Bulanık AHP önem tablosu (Rao'dan (2008) uyarlanmıştır)

Linguistik İfade	Bulanık Sayılar	Ters Bulanık Sayılar
Eşit Önemde	(1, 1, 3)	(1/3, 1, 1)
Biraz Daha Önemli (Az Üstünlük)	(1, 3, 5)	(1/5, 1/3, 1)
Oldukça Önemli (Fazla Üstünlük)	(3, 5, 7)	(1/7, 1/5, 1/3)
Çok Önemli (Çok Üstünlük)	(5, 7, 9)	(1/9, 1/7, 1/5)
Son Derece Önemli (Kesin Üstünlük)	(7, 9, 9)	(1/9, 1/9, 1/7)

Bulanık AHP sübjektif değerlendirmelerle ilgili karar verme problemlerinin çözümü için geliştirilmiştir ve seçim ve değerlendirme ile ilgili konularda başta TOPSIS, QFD, Delphi ve ANP gibi diğer yöntemlerle birlikte kullanımını gösteren birçok çalışma bulunmaktadır (Emrouznejad ve Ho, 2018: 7-8).

2.7.6. ELECTRE (Elimination et Choix Traduisant La Realite) Metodu

Çok Kriterli Karar Verme metotlarından bir diğeri olan ELECTRE'nin temelleri 1965 yılında, SEMA adlı Avrupa danışmanlık firmasında atılmıştır. Metot, o dönemde şirketlerde yeni faaliyetlerin geliştirilmesi ile ilgili karar verme konusundaki bir gerçek dünya problemi üzerinde çalışan bir ekibin kullandığı MARSAN (Méthode d'Analyse, de Recherche, et de Sélection d'Activités Nouvelles) metodundaki bazı problemlerin fark edilmesi ve daha sonra bu kısıtlılıkların üstesinden gelmek için ekip üyelerinden Bernard Roy'un önerdiği yeni bir metoda dayanmaktadır (Figueira, Mousseau ve Roy, 2005).

ELECTRE metodunun temeli de diğer Çok Kriterli Karar Verme metotlarına benzer biçimde alternatifler arasında bir üstünlük ilişkisi kurulmasına dayanmaktadır. ELECTRE metodu ile yapılan hesaplama işlemleri sekiz adımdan oluşmaktadır. Bu işlem adımları kısaca aşağıda verilmiş, ayrıca her bir adım dört kritere göre beş blokzincir platform alternatifinin seçim kararı için örneklendirilmiştir.

Adım 1. Karar matrisinin (A) oluşturulması: Karar matrisi olarak adlandırılan başlangıç matrisi Eş. 2.11'de verildiği biçimde oluşturulur. Bu matrisin satırları alternatifler, sütunları ise karar vermek için kullanılacak kriterleri içerir. Buna göre, 'm' alternatif sayısı, 'n' ise kriter sayısıdır.

$$A_{ij} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ . & . & & . \\ . & . & & . \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix} \quad (2.11)$$

Buna göre, beş alternatif blokzincir platformunun dört kritere göre özelliklerini içeren matris Çizelge 2.61'de verilmiştir.

Çizelge 2.61. Blokzincir platformu alternatifleri için ilgili kriter değerleri ve kriter ağırlıkları – ELECTRE metodu

Kriter	**İşlem hacmi (saniyede işlem)**	**İşlem hızı (saniye)**	**Olgunluk düzeyi (1-5 aralığında)**	**Popülarite (1-5 aralığında)**
Fayda/maliyet	**Fayda**	**Maliyet**	**Fayda**	**Fayda**
Ağırlık / Alternatif	**0,3**	**0,2**	**0,25**	**0,25**
Ethereum	20	15	5	5
Hyperledger Fabric	3 500	1	3	4
Quorum	1 000	1	3	3
Corda	20 000	1	3	2
IOTA	10 000	12	2	3

Çizelge 2.61'de her bir kriter ayrıca fayda ve maliyet olarak sınıflandırılmıştır. Fayda ifadesi değerinin yüksek olması istenen kriterleri, maliyet ise değerinin düşük olması istenen kriterleri ifade etmektedir.

Adım 2. Normalize edilmiş karar matrisinin (X) oluşturulması: X matrisi, ilk adımda oluşturulan A matrisinin elemanları kullanılarak oluşturulan matristir. Kriterlerin fayda ve maliyet özelliği taşımasına göre iki farklı normalizasyon formülü kullanılmaktadır. Eş. 2.12'de maliyet kriterinin, Eş. 2.13'te ise fayda kriterinin normalizasyon formülü verilmiştir.

$$x_{ij} = \frac{1/a_{ij}}{\sqrt{\sum_{i=1}^{m}\left(\frac{1}{a_{ij}}\right)^2}} \qquad \begin{matrix}(i = 1, 2, \dots, m)\\(j = 1, 2, \dots, n)\end{matrix} \tag{2.12}$$

$$x_{ij} = \frac{a_{ij}}{\sqrt{\sum_{i=1}^{m}(a_{ij})^2}} \qquad \begin{matrix}(i = 1, 2, \dots, m)\\(j = 1, 2, \dots, n)\end{matrix} \tag{2.13}$$

Yukarıdaki Eş. 2.12 ve 2.13 kullanılarak yapılan hesaplamalar sonucunda aşağıda verilmiş olan Eş. 2.14 elde edilmektedir.

$$X_{ij} = \begin{bmatrix} x_{11} & x_{12} & \dots & x_{1n} \\ x_{21} & x_{22} & \dots & x_{2n} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ x_{m1} & x_{m2} & \dots & x_{mn} \end{bmatrix} \tag{2.14}$$

Çizelge 2.61'de verilen karar matrisi fayda ve maliyet kriterleri için verilen formüller kullanılarak normalize edilmiş, sonuçta Çizelge 2.62'de verilmiş olan hesaplama değerlerine göre Çizelge 2.63'te verilmiş olan normalize karar matrisi elde edilmiştir.

Çizelge 2.62. Blokzincir platformu alternatifleri için normalize karar matrisi hesaplamaları – ELECTRE metodu

	Fayda	**Maliyet**	**Fayda**	**Fayda**
Ağırlık	**0,3**	**0,2**	**0,25**	**0,25**
Kriter	**İşlem hacmi (a_{ij}^2)**	**İşlem hızı (saniye – $1/a_{ij}^2$)**	**Olgunluk düzeyi (a_{ij}^2)**	**Popülarite (a_{ij}^2)**
Ethereum	400	0,004444444	25	25
Hyperledger Fabric	12250000	1	9	16
Quorum	1000000	1	9	9
Corda	400000000	1	9	4
IOTA	100000000	0,006944444	4	9
Toplam	513250400	3,011388889	56	63
Karekök	22655,03035	1,735335382	7,483314774	7,937253933

Çizelge 2.63. Blokzincir platformu alternatifleri için normalize karar matrisi – ELECTRE metodu

	Fayda	**Maliyet**	**Fayda**	**Fayda**
Ağırlık	**0,3**	**0,2**	**0,25**	**0,25**
Kriter	**İşlem hacmi (saniyede işlem)**	**İşlem hızı (saniye)**	**Olgunluk düzeyi (1-5 aralığında)**	**Popülarite (1-5 aralığında)**
Ethereum	0,000882806	0,038417166	0,668153105	0,629940788
Hyperledger Fabric	0,154491075	0,576257483	0,400891863	0,503952631
Quorum	0,044140307	0,576257483	0,400891863	0,377964473
Corda	0,882806145	0,576257483	0,400891863	0,251976315
IOTA	0,441403072	0,048021457	0,267261242	0,377964473

Adım 3. Ağırlıklı normalize karar matrisinin (V) oluşturulması: V matrisinin oluşturulması için öncelikle kriterlerin ağırlıkları belirlenir. Doğal olarak, kriterlerin ağırlıkları toplamı bire eşittir. Ağırlıklar belirlendikten sonra bu ağırlıklar X matrisi ile çarpılarak Eş. 2.15'te verilmiş olan V matrisi bulunur.

$$V_{ij} = \begin{bmatrix} w_1x_{11} & w_2x_{12} & \dots & w_nx_{1n} \\ w_1x_{21} & w_2x_{22} & \dots & w_nx_{2n} \\ . & . & . & \\ . & . & . & \\ w_1x_{m1} & w_2x_{m2} & \dots & w_nx_{mn} \end{bmatrix} \quad (2.15)$$

Örnek uygulama için oluşturulmuş olan ağırlıklı normalize karar matrisi Çizelge 2.64'te verilmiştir.

Çizelge 2.64. Blokzincir platformu alternatifleri için ağırlıklı normalize karar matrisi – ELECTRE metodu

Ağırlık (w)	**0,3**	**0,2**	**0,25**	**0,25**
Kriter	**İşlem hacmi (saniyede işlem)**	**İşlem hızı (saniye)**	**Olgunluk düzeyi (1-5 aralığında)**	**Popülarite (1-5 aralığında)**
Ethereum	0,000264842	0,007683433	0,167038276	0,157485197
Hyperledger Fabric	0,046347323	0,115251497	0,100222966	0,125988158
Quorum	0,013242092	0,115251497	0,100222966	0,094491118
Corda	0,264841843	0,115251497	0,100222966	0,062994079
IOTA	0,132420922	0,009604291	0,06681531	0,094491118

Adım 4. Uyum ve uyumsuzluk kümelerinin belirlenmesi: Uyum kümeleri V matrisi kullanılarak belirlenir. İkili karar noktalarının karşılaştırılması için kriterler iki ayrı küme biçiminde ayrılır. Satırlarda yer alan elemanlar, yani alternatifler bu matristeki değerlerine göre birbirleriyle karşılaştırılır. Bu karşılaştırma sonucunda, karşılaştırılan alternatifin değeri diğer alternatiften daha büyük ise değerinin yer aldığı sütun indisi uyum kümesine, aksi halde uyumsuzluk kümesine dâhil edilir. Burada, uyum kümesi C_{pq}, uyumsuzluk kümesi de D_{pq} olmak üzere A_p ve A_q (1, 2, …,m ve p≠q) uyum kümesinde A_p alternatifinin A_q alternatifine tercih edildiği kriterlerin kümesi C_{pq}'dur. Her uyum kümesinin karşılığı olarak bir uyumsuzluk kümesi bulunur ve bu kümeler birbirlerinin tümleyenidir.

Çoklu karar problemlerinde uyum kümesi sayısı, 'm' alternatif ya da satır sayısı olmak üzere (m_xm – m) adettir.

'j' sütun indeksi ya da kriter sıra numarası, 'k' satır indeksi ya da alternatif sıra numarası, y_{kj} k. alternatifin j. kritere göre değeri, 'n' kriter sayısı ve 'm' alternatif sayısı olmak üzere, uyum kümesi Eş 2.16 ile, uyumsuzluk kümesi ise Eş. 2.17 ile ifade edilmektedir.

$$C_{kl} = \{j,\ y_{kj} \geq y_{lj} \mid j = 1,2,\dots,n\} \tag{2.16}$$

$$D_{kl} = \{j,\ y_{kj} < y_{lj} \mid j = 1,2,\dots,n\} \tag{2.17}$$

Çizelge 2.66'te verilmiş olan ağırlıklı normalize karar matrisine göre uyum ve uyumsuzluk kümeleri Çizelge 2.65'te verilmiştir. Çizelge 2.64'te yer verilmiş olan 'C_{12}' Ethereum ile Hyperledger Fabric karşılaştırmasını ifade etmektedir. Tüm platformların birbirleri ile karşılaştırılması sonucunda bulunan küme sayısı 'm x m – m' eşitliğinden hareketle 20'dir (5x5-5). 'n' kriter sayısı olan dört olmak üzere uyum ve tümleyeni olan uyumsuzluk kümelerinin eleman sayıları toplamı ise dörttür. Bu kümenin elemanları için, '1' işlem hacmini, '2' işlem hızını, '3' olgunluk düzeyini, '4' ise popülariteyi ifade etmektedir.

Çizelge 2.65. Blokzincir platformu alternatifleri için uyum ve uyumsuzluk kümeleri – ELECTRE metodu

Uyum kümeleri		**Uyumsuzluk kümeleri**	
C_{12}=	{3,4}	D_{12}=	{1,2}
C_{13}=	{3,4}	D_{13}=	{1,2}
C_{14}=	{3,4}	D_{14}=	{1,2}
C_{15}=	{3,4}	D_{15}=	{1,2}
C_{21}=	{1,2}	D_{21}=	{3,4}
C_{23}=	{1,2,3,4}	D_{23}=	{ }
C_{24}=	{2,3,4}	D_{24}=	{1}
C_{25}=	{2,3,4}	D_{25}=	{1}
C_{31}=	{1,2}	D_{31}=	{3,4}
C_{32}=	{2,3}	D_{32}=	{1,4}
C_{34}=	{2,3,4}	D_{34}=	{1}
C_{35}=	{2,3,4}	D_{35}=	{1}
C_{41}=	{1,2}	D_{41}=	{3,4}
C_{42}=	{1,2,3}	D_{42}=	{4}
C_{43}=	{1,2,3}	D_{43}=	{4}
C_{45}=	{1,2,3}	D_{45}=	{4}
C_{51}=	{1,2}	D_{51}=	{3,4}
C_{52}=	{1}	D_{52}=	{2,3,4}
C_{53}=	{1,4}	D_{53}=	{2,3}
C_{54}=	{4}	D_{54}=	{1,2,3}

Adım 5. Uyum ve uyumsuzluk matrislerinin oluşturulması: Dördüncü adımda belirlenmiş olan uyum ve uyumsuzluk kümeleri kullanılarak bu matrisler hesaplanmaktadır. Bu matrisler alternatif sayısının boyutundadır (yani mxm). Uyum matrisinin elemanları Eş. 2.18'e göre hesaplanır. Uyum matrisinin elemanları uyum endeksi olarak da adlandırılır.

$$c_{kl} = \sum_{j \in C_{kl}} w_j \,, \qquad j = 1,2,\dots,n \tag{2.18}$$

Uyumsuzluk matrisinin elemanları ise A_k alternatifinin A_l alternatifine göre daha kötü olma durumunu ifade etmektedir. Uyumsuzluk matrisinin elemanları ise Eş. 2.19'a göre hesaplanmaktadır.

$$d_{kl} = \frac{max|y_{kj} - y_{lj}|, j \in D_{kl}}{max|y_{kj} - y_{lj}|, \forall j} \quad (2.19)$$

Çizelge 2.65'te verilmiş olan uyum ve uyumsuzluk kümelerine bu formüller uygulanarak uyum ve uyumsuzluk matrislerinin elemanları Çizelge 2.66'da verildiği biçimde hesaplanmıştır (w_1=0,3; w_2=0,2; w_3=0,25; w_4=0,25).

Çizelge 2.66. Blokzincir platformu alternatifleri için uyum ve uyumsuzluk matrislerinin elemanları – ELECTRE metodu

Uyum kümeleri		**w_1=0,30; w_2=0,20; w_3=0,25; w_4=0,25**	**Uyumsuzluk kümeleri**		**w_1=0,30; w_2=0,20; w_3=0,25; w_4=0,25**
C_{12}=	{3,4}	0,25+0,25=0,50	D_{12}=	{1,2}	$\frac{max\|(0{,}0461), (\mathbf{0}, \mathbf{1076})\|}{max\|(0{,}0461), (\mathbf{0}, \mathbf{1076}), (0{,}0668), (0{,}0315)\|}$
C_{13}=	{3,4}	0,25+0,25=0,50	D_{13}=	{1,2}	0,1076/0,1076 =1
C_{14}=	{3,4}	0,25+0,25=0,50	D_{14}=	{1,2}	0,2646/0,2646=1
C_{15}=	{3,4}	0,25+0,25=0,50	D_{15}=	{1,2}	0,1322/0,1322=1
C_{21}=	{1,2}	0,30+0,20=0,50	D_{21}=	{3,4}	0,0668/0,1076=0,62
C_{23}=	{1,2,3,4}	0,30+0,20+0,25+0,25=1	D_{23}=	{ }	0
C_{24}=	{2,3,4}	0,20+0,25+0,25=0,70	D_{24}=	{1}	0,2185/0,2185=1
C_{25}=	{2,3,4}	0,20+0,25+0,25=0,70	D_{25}=	{1}	0,0861/0,1056=0,8147
C_{31}=	{1,2}	0,30+0,20=0,50	D_{31}=	{3,4}	0,0668/0,1076=0,62
C_{32}=	{2,3}	0,20+0,25=0,45	D_{32}=	{1,4}	0,03311/0,03311=1
C_{34}=	{2,3,4}	0,20+0,25+0,25=0,70	D_{34}=	{1}	0,2515/0,2515=1
C_{35}=	{2,3,4}	0,20+0,25+0,25=0,70	D_{35}=	{1}	0,1192/0,1192=1
C_{41}=	{1,2}	0,30+0,20=0,50	D_{41}=	{3,4}	0,0945/0,2646=0,357
C_{42}=	{1,2,3}	0,30+0,20+0,25=0,75	D_{42}=	{4}	0,063/0,218=0,2883
C_{43}=	{1,2,3}	0,30+0,20+0,25=0,75	D_{43}=	{4}	0,0315/0,2516=0,1252
C_{45}=	{1,2,3}	0,30+0,20+0,25=0,75	D_{45}=	{4}	0,0315/0,1324=0,238
C_{51}=	{1,2}	0,30+0,20=0,50	D_{51}=	{3,4}	0,1002/0,1322=0,7584
C_{52}=	{1}	0,30	D_{52}=	{2,3,4}	0,106/0,106=1
C_{53}=	{1,4}	0,55	D_{53}=	{2,3}	0,106/0,1191=0,8865
C_{54}=	{4}	0,25	D_{54}=	{1,2,3}	0,1324/0,1324=1

Çizelge 2.66'ya göre oluşturulan uyum matrisi çizelge 2.67'de, uyumsuzluk matrisi ise Çizelge 2.68'de verilmiştir.

Çizelge 2.67. Blokzincir platformu alternatifleri için uyum matrisi – ELECTRE metodu

	Ethereum	**Hyperledger Fabric**	**Quorum**	**Corda**	**IOTA**
Ethereum	-	0,50	0,50	0,50	0,50
Hyperledger Fabric	0,50	-	1	0,70	0,70
Quorum	0,50	0,45	-	0,70	0,70
Corda	0,50	0,75	0,75	-	0,75
IOTA	0,50	0,30	0,55	0,25	-

Çizelge 2.68. Blokzincir platformu alternatifleri için uyumsuzluk matrisi – ELECTRE metodu

	Ethereum	**Hyperledger Fabric**	**Quorum**	**Corda**	**IOTA**
Ethereum	-	1	1	1	1
Hyperledger Fabric	0,62	-	0	1	0,8147
Quorum	0,62	1	-	1	1
Corda	0,357	0,2883	0,1252	-	0,238
IOTA	0,7584	1	0,8865	1	-

Adım 6. Uyum (C) ve uyumsuzluk (D) üstünlükleri matrislerinin oluşturulması: Bu adımda uyum ve uyumsuzluk matrisleri için eşik değerler belirlenir. Üstünlük matrisleri bu eşik değerler kullanılarak oluşturulur. 'm' alternatif sayısı, 'c_{kl}' uyum endeksi, 'd_{kl}' uyumsuzluk endeksi olmak üzere uyum eşik değeri Eş. 2.20'ye, uyumsuzluk eşik değeri ise Eş. 2.21'e göre hesaplanmaktadır.

$$\underline{c} = \frac{1}{m(m-1)} \sum_{k=1}^{m} \sum_{l=1}^{m} c_{kl}\,, k \neq l \; ve \; l \neq k \tag{2.20}$$

$$\underline{d} = \frac{1}{m(m-1)} \sum_{k=1}^{m} \sum_{l=1}^{m} d_{kl}, k \neq l \; ve \; l \neq k \tag{2.21}$$

Bulunan bu eşik değerler uyum ve uyumsuzluk matrislerindeki değerlerle karşılaştırılır. 'c_{kl}' ve 'd_{kl}' için bulunan eşik değerlerden büyük olanlara '1', küçük olanlara ise '0' değeri verilir. Böylece uyum ve uyumsuzluk üstünlük matrisleri oluşturulur.

Blokzincir platformlarına ilişkin örnek için uyum ve uyumsuzluk matrisleri eşik değerleri aşağıdaki biçimdedir:

Uyum eşik değeri;

$$\frac{1}{5x(5-1)}(0{,}5 + 0{,}5 + 0{,}5 + 0{,}5 + 0{,}5 + 1 + 0{,}7 + 0{,}7 + 0{,}5 + 0{,}45 + 0{,}7 + 0{,}7 + 0{,}5$$
$$+ 0{,}75 + 0{,}75 + 0{,}75 + 0{,}5 + 0{,}3 + 0{,}55 + 0{,}25) = \frac{11{,}6}{20} = \mathbf{0,58}$$

Uyumsuzluk eşik değeri;

$$\frac{1}{5x(5-1)}(1+1+1+1+0{,}62+0+1+0{,}8147+0{,}62+1+1+1+0{,}7584+1$$
$$+0{,}8865+1)=\frac{14{,}71}{20}=\mathbf{0,735}$$

Bu eşik değerlere göre uyum matrisi düzenlenerek Çizelge 2.69'da verilmiş olan uyum üstünlük matrisi oluşturulmuştur.

Çizelge 2.69. Blokzincir platformu alternatifleri için uyum üstünlük matrisi – ELECTRE metodu

	Ethereum	**Hyperledger Fabric**	**Quorum**	**Corda**	**IOTA**
Ethereum	-	0	0	0	0
Hyperledger Fabric	0	-	1	1	1
Quorum	0	0	-	1	1
Corda	0	1	1	-	1
IOTA	0	0	0	0	-

Uyumsuzluk eşik değerine göre hazırlanmış olan uyumsuzluk üstünlük matrisi ise Çizelge 2.70'te verilmiştir.

Çizelge 2.70. Blokzincir platformu alternatifleri için uyumsuzluk üstünlük matrisi – ELECTRE metodu

	Ethereum	**Hyperledger Fabric**	**Quorum**	**Corda**	**IOTA**
Ethereum	-	1	1	1	1
Hyperledger Fabric	0	-	0	1	1
Quorum	0	1	-	1	1
Corda	0	0	0	-	0
IOTA	1	1	1	1	-

Adım 7. Baskınlık matrisinin oluşturulması: Bu adımda, uyum üstünlük matrisi ile uyumsuzluk üstünlük matrisinin değerleri çarpılarak toplam baskınlık matrisi oluşturulur. Bu çarpma işlemi bir matris çarpımı değil, aynı satır ve sütun indislerine sahip iki matris elemanının birbiri ile çarpılması biçimindedir. 'E' baskınlık matrisi, 'e_{kl}' bu matrisin elemanları, 'f_{kl}' uyum üstünlük matrisinin elemanı, 'g_{kl}' uyumsuzluk üstünlük matrisinin elemanı olmak üzere, bu matrisin elemanları Eş. 2.22'ye göre hesaplanır.

$$e_{kl} = f_{kl} x\, g_{kl} \tag{2.22}$$

Çizelge 2.69 ve 2.70'te verilmiş olan üstünlük matrislerinin elemanlarının birbirleri ile çarpılmasıyla bulunan baskınlık matrisi Çizelge 2.71'de verilmiştir.

Çizelge 2.71. Blokzincir platformu alternatifleri için baskınlık matrisi – ELECTRE metodu

	Ethereum	**Hyperledger Fabric**	**Quorum**	**Corda**	**IOTA**
Ethereum	-	0x1	0x1	0x1	0x1
Hyperledger Fabric	0x0	-	1x0	1x1	1x1
Quorum	0x0	0x1	-	1x1	1x1
Corda	0x0	1x0	1x0	-	1x0
IOTA	0x1	0x1	0x1	0x1	-

Adım 8. Alternatiflerin önem sırasının belirlenmesi: Bir önceki adımda oluşturulmuş olan matris kullanılarak kısmi tercih sıralaması yapılabilmektedir. 'E' baskınlık matrisinde e_{kl}'nin bire eşit olması A_k alternatifinin A_l alternatifine göre daha tercih edildiği anlamına gelmektedir. Baskınlık matrisinde bir sütundaki elemanın bire eşit olması ilgili satırdaki alternatifin o sütundaki alternatiften üstün olduğunu göstermektedir. Çizelge 2.71'deki baskınlık matrisinde yer verilen çarpımlar yapıldığında Çizelge 2.72'de verilmiş olan nihai baskınlık matrisi elde edilmektedir.

Çizelge 2.72. Blokzincir platformu alternatifleri için nihai baskınlık matrisi – ELECTRE metodu

	Ethereum	**Hyperledger Fabric**	**Quorum**	**Corda**	**IOTA**
Ethereum	-	0	0	0	0
Hyperledger Fabric	0	-	0	1	1
Quorum	0	0	-	1	1
Corda	0	0	0	-	0
IOTA	0	0	0	0	-

Çizelge 2.72'de verilmiş olan baskınlık matrisine göre aşağıdaki çıkarımlar yapılmaktadır:

- Ethereum, Corda ve IOTA'nın hiçbir platforma karşı üstünlüğü bulunmaktadır.
- Hayperledger, Corda ve IOTA'ya üstündür.
- Quorum, Corda ve IOTA'ya üstündür.

ELECTRE metoduna göre Hyperledger ve Quorum platformları diğer platformlara göre üstün olmakla birlikte bu iki platformun birbirlerine karşı üstünlükleri bulunmamaktadır. İkili karşılaştırmalara bakıldığında işlem hacmi ve popülarite bakımından daha üstün olan Hyperledger'in seçilmesi uygundur.

2.7.7. TOPSIS (Technique for Order of Preference by Similarity to Ideal Solution) Metodu

En iyi çözüme yakınlık ve en kötü çözüme uzaklık temeline dayalı bir Çok Kriterli Karar Verme metodudur. Diğer ÇKKV metotlarına benzer biçimde TOPSIS'te de her bir kriter için ağırlıklar belirlendikten sonra kriter değerlerini içeren matris normalleştirilir. Diğerlerinden farklı olarak, TOPSİS'te her bir alternatifin her bir kriterdeki en iyi ve en kötü alternatife geometrik yakınlığı hesaplanır. TOPSİS metodunun işlem adımları aşağıda verilmiştir. Bu adımlar ayrıca beş blokzincir platform alternatifinin dört kritere göre seçim kararı için örneklendirilmiştir.

Adım 1. Karar matrisinin oluşturulması: Diğer metotlara benzer biçimde, ilk adımda sütunlarında kriterlerin, satırlarında ise alternatiflerin olduğu karar matrisi oluşturulur. 'n' sayıda kriter ve 'm' sayıda alternatif için oluşturulmuş olan A_{ij} karar matrisi Eş. 2.23'te verilmiştir.

$$A_{ij} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ . & . & & . \\ . & . & & . \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix} \quad (2.23)$$

Beş alternatif blokzincir platformunun dört kritere göre özelliklerini içeren matris Çizelge 2.73'te verilmiştir.

Çizelge 2.73. Blokzincir platformu alternatifleri için ilgili kriter değerleri ve kriter ağırlıkları – TOPSIS metodu

Kriter	**İşlem hacmi (saniyede işlem)**	**İşlem hızı (saniye)**	**Olgunluk düzeyi (1-5 aralığında)**	**Popülarite (1-5 aralığında)**
Fayda/maliyet	**Fayda**	**Maliyet**	**Fayda**	**Fayda**
Ağırlık / Alternatif	**0,3**	**0,2**	**0,25**	**0,25**
Ethereum	20	15	5	5
Hyperledger Fabric	3 500	1	3	4
Quorum	1 000	1	3	3
Corda	20 000	1	3	2
IOTA	10 000	12	2	3

Adım 2. Normalize karar matrisinin oluşturulması: İlk adımda oluşturulmuş olan karar matrisi Eş. 2.24 kullanılarak '$R = (r_{ij})_{mxn}$' normalize edilmiş matrisi oluşturulur.

$$r_{ij} = \frac{a_{ij}}{\sqrt{\sum_{i=1}^{m} a_{ij}^2}} \quad i = 1, \dots, m \,; j = 1, \dots, n \tag{2.24}$$

Eş. 2.24'e göre hesaplanmış olan normalize karar matrisi Çizelge 2.74'te verilmiştir.

Çizelge 2.74. Blokzincir platformu alternatifleri için normalize karar matrisi – TOPSIS metodu

Kriter	**İşlem hacmi (saniyede işlem)**	**İşlem hızı (saniye)**	**Olgunluk düzeyi (1-5 aralığında)**	**Popülarite (1-5 aralığında)**
Fayda/maliyet	**Fayda**	**Maliyet**	**Fayda**	**Fayda**
Ağırlık / Alternatif	**0,3**	**0,2**	**0,25**	**0,25**
Ethereum	0,00088	0,77771	0,66815	0,62994
Hyperledger Fabric	0,15449	0,05185	0,40089	0,50395
Quorum	0,04414	0,05185	0,40089	0,37796
Corda	0,88281	0,05185	0,40089	0,25198
IOTA	0,44140	0,62217	0,26726	0,37796

Adım 3. Ağırlıklı normalize karar matrisinin oluşturulması: Bu adımda, ikinci adımda oluşturulmuş olan normalize karar matrisinin elemanları her bir kriterin ağırlığı (w_{ij}) ile çarpılır.

Çizelge 2.75'te örnek karar matrisi elemanlarının kriter ağırlıkları ile çarpılması sonucunda bulunan ağırlıklı normalize karar matrisi verilmiştir.

Çizelge 2.75. Blokzincir platformu alternatifleri için ağırlıklı normalize karar matrisi – TOPSIS metodu

Kriter	**İşlem hacmi (saniyede işlem)**	**İşlem hızı (saniye)**	**Olgunluk düzeyi (1-5 aralığında)**	**Popülarite (1-5 aralığında)**
Fayda/maliyet	**Fayda**	**Maliyet**	**Fayda**	**Fayda**
Ağırlık / Alternatif	**0,3**	**0,2**	**0,25**	**0,25**
Ethereum	0,00026	0,15554	0,16704	0,15749
Hyperledger Fabric	0,04635	0,01037	0,10022	0,12599
Quorum	0,01324	0,01037	0,10022	0,09449
Corda	0,26484	0,01037	0,10022	0,06299
IOTA	0,13242	0,12443	0,06682	0,09449

Adım 4. En iyi ve en kötü alternatiflerin bulunması: A_b en iyi alternatif A_w en kötü alternatif olmak üzere, her bir kriter (sütun) için en iyi ve en kötü elemanlar bulunur. Burada, ilgili kriterin fayda kriteri mi maliyet kriteri mi olduğuna dikkat edilmelidir. 'v_{ij}' ağırlıklı normalize karar matrisinin elemanı olmak üzere, bu alternatifler aşağıda verilmiş olan Eş. 2.25 ve 2.26 kullanılarak bulunur.

$$A_b = \{(\max v_{ij}\ j \in J), (\min v_{ij}\ j \in J')\} \tag{2.25}$$

$$A_w = \{(\min v_{ij}\ j \in J), (\max v_{ij}\ j \in J')\} \tag{2.26}$$

Bu eşitliklerde 'J' fayda kriterini, 'J'' ise maliyet kriterini ifade etmektedir.

Blokzincir platform alternatifleri örneği için Eşitlik 2.25 ve 2.26 kullanılarak bulunan en iyi ve en kötü alternatif değerleri Çizelge 2.76'da gösterilmiştir. Burada, 'işlem hızı' kriterinin düşük değerli olması istendiği için bir maliyet kriteri olduğu gözden kaçırılmamalıdır.

Çizelge 2.76. En iyi ve en kötü alternatif değerleri – TOPSIS metodu

Kriter	**İşlem hacmi (saniyede işlem)**	**İşlem hızı (saniye)**	**Olgunluk düzeyi (1-5 aralığında)**	**Popülarite (1-5 aralığında)**
Fayda/maliyet	**Fayda**	**Maliyet**	**Fayda**	**Fayda**
A_b	0,26484	0,01037	0,16704	0,15749
A_w	0,00026	0,15554	0,06682	0,06299

Adım 5. Öklid mesafesinin hesaplanması: Her bir alternatifin ideal (en iyi) ve en kötü çözüme uzaklığı Öklid uzaklık formülü kullanılarak hesaplanır. 'S_i^+' ve 'S_i^-' sırasıyla en iyi çözüme ve en kötü çözüme uzaklık ölçüsü olmak üzere bu mesafeler Eş. 2.27 ve 2.28 kullanılarak hesaplanır.

$$S_i^+ = \sqrt{\sum_{j=1}^{n} \left(v_{ij} - A_b\right)^2}, i = 1,2, \dots, m \tag{2.27}$$

$$S_i^- = \sqrt{\sum_{j=1}^{n} \left(v_{ij} - A_w\right)^2}, i = 1,2, \dots, m \tag{2.28}$$

Çizelge 2.77'de Çizelge 2.76'daki değerler ile Eş. 2.27 ve 2.28 kullanılarak hesaplanmış olan Öklid mesafeleri verilmiştir.

Çizelge 2.77. Blokzincir alternatifleri için Öklid mesafeleri – TOPSIS metodu

	S_i^+	S_i^-
Ethereum	0,3098	0,1377
Hyperledger Fabric	0,2355	0,1682
Quorum	0,2752	0,1528
Corda	0,1157	0,3116
IOTA	0,2118	0,1405

Adım 6. Performans skorunun (ideal çözüme göreli yakınlığın) hesaplanması: A_i alternatifinin performans skoru olan P_i Eş. 2.29'a göre hesaplanır.

$$P_i = \frac{S_i^-}{(S_i^- + S_i^+)}, \quad i = 1,2,\dots,m \tag{4.29}$$

Blokzincir platform alternatifleri için Eş. 2.29'a göre hesaplanmış olan performans skorları Çizelge 2.78'de verilmiştir.

Çizelge 2.78. Blokzincir alternatifleri için performans skorları – TOPSIS metodu

	Performans Skoru
Ethereum	0,3078
Hyperledger Fabric	0,4166
Quorum	0,3570
Corda	**0,7292**
IOTA	0,3987

Adım 7. Alternatiflerin performans skoruna göre sıralanması: bu adımda, bir önceki adımda hesaplanmış olan performans skorlarına göre alternatifler büyükten küçüğe sıralanır.

Çizelge 2.78'de verilmiş olan performans skorlarına göre blokzincir platform alternatiflerinin sıralaması Corda, Hyperledger Fabric, IOTA, Quorum ve Ethereum biçimindedir.

2.7.8. Çok Kriterli Karar Verme metotlarının karşılaştırılması

Yukarıda açıklanmış olan metotlar kullanılarak hesaplanmış olan blokzincir platform alternatiflerinin öncelik sıralaması her bir metot için Çizelge 2.79'da verilmiştir.

Çizelge 2.79. Tüm metotlara göre blokzincir platform alternatiflerinin öncelik sıralaması

	Ağırlıklandırılmış Toplam Modeli	**Ağırlıklandırılmış Çarpım Modeli**	**AHP**	**ELECTRE**	**TOPSIS**
1	Corda	Corda	Corda	Hyperledger Fabric	Corda
2	Hyperledger Fabric	Hyperledger Fabric	IOTA	Quorum	Hyperledger Fabric
3	Quorum	IOTA	Hyperledger Fabric	Corda	IOTA
4	Ethereum	Quorum	Quorum	IOTA	Quorum
5	IOTA	Ethereum	Ethereum	Ethereum	Ethereum

Buna göre, beş metottan dördünde Corda alternatifi ilk sıradadır. Alternatifler içerisinde en kötü olanlar ise genel olarak Ethereum ve Quorum'dur.

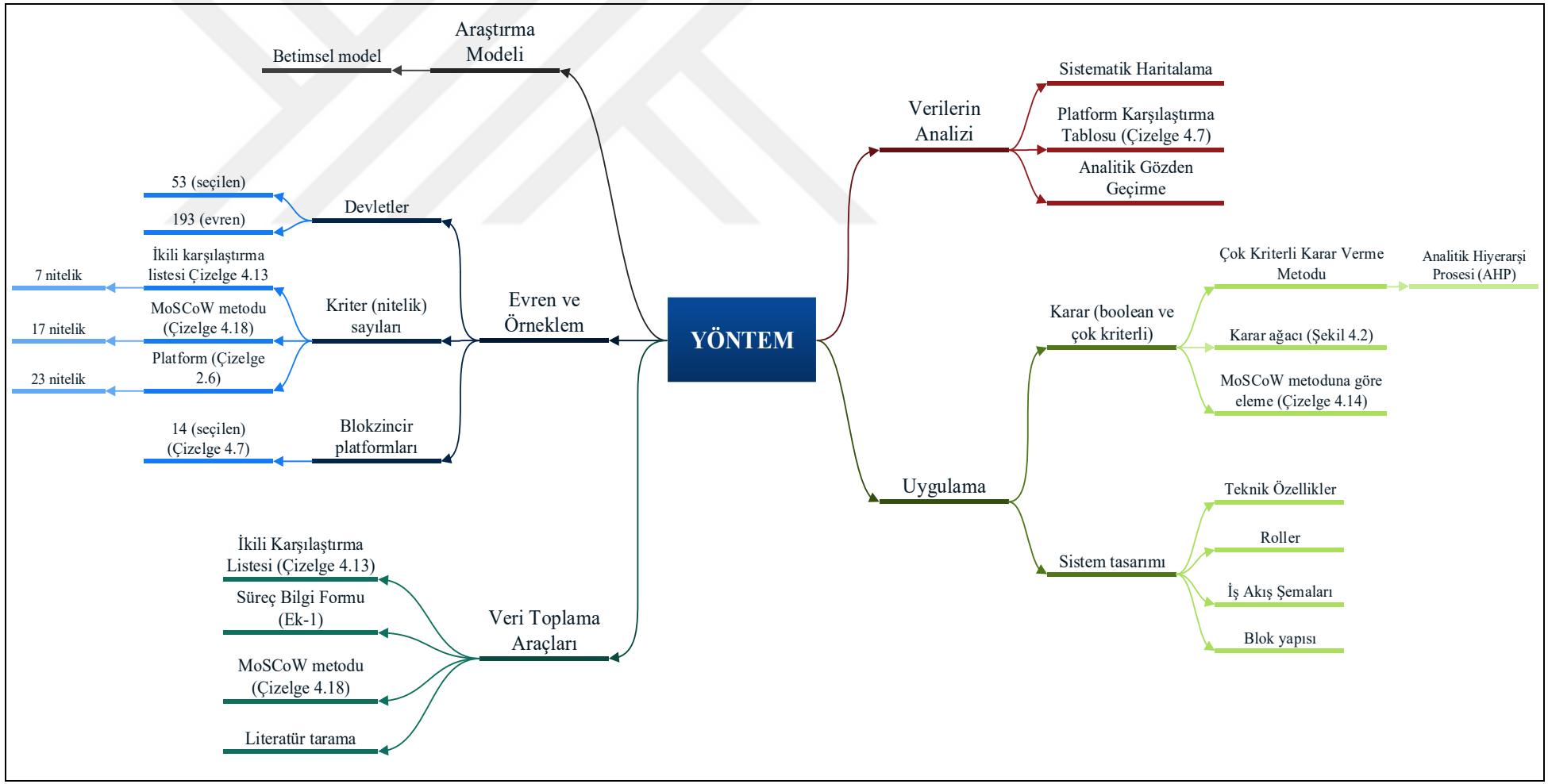
3. YÖNTEM

Bu çalışmada, blokzincir teknolojisinin herhangi bir kamu hizmet sürecinin yürütülmesinde kullanılması kararına yardımcı olacak bir model geliştirilmesi hedeflenmiştir. Önerilen model, blokzincir çözümüne ilişkin birden fazla karar noktasını, çoklu değerlendirmeleri, yönlendirmeleri, alternatifleri ve bilgi formlarını içeren bir karar destek sistemidir.

Karar verme en temel anlamıyla bir hedef ya da sorunun belirlenerek, gerekli bilgiler toplanarak ve alternatif çözümler değerlendirilerek seçim yapma sürecidir (Panpatte ve Takale, 2019). Yönetim bilimleri alanında önde gelen isimlerden George R. Terry ise karar vermeyi iki veya daha fazla olası alternatif arasından bazı kriterlere dayalı olarak seçim yapmak olarak tanımlamaktadır.

Gerek en basit gerekse en karmaşık hali ile karar verme süreci temelde benzer işlem adımlarını izlemektedir. Bu adımlar karar verilecek konu ya da sorunun tanımlanması, bilgi toplama, alternatiflerin belirlenmesi, alternatiflerin değerlendirilmesi, kararın verilmesi ve verilen kararın daha sonra gözden geçirilmesi biçimindedir. Gerek karar vermede, gerekse karar vericilere yardımcı karar destek sistemlerinin tasarlanmasında karar kalitesi doğrudan veri ve bilginin ilgililiğine, yeterliliğine, güvenilirliğine ve erişilebilirliğine bağlıdır. Blokzincir teknolojisinin kullanımına ilişkin kararlar da bu bağlamda çok ve çeşitli bilgiye ve veriye gereksinim duymakta, ihtiyaç duyulan bu bilgilerin bir kısmını da teknik ve anlaşılması güç konular oluşturmaktadır. Bu nedenle, bu tez çalışmasında detaylı analiz ve bilgi toplama gerektiren konular öncelikle sistematik bir biçimde derlenerek analiz edilmiş, analiz sonuçlarından kurallar oluşturulmuş, bu kurallara dayalı hesaplama işlemleri ile çözüm alternatiflerinin değerlendirilmesine ilişkin yöntem tarif edilmiştir.

Tezin hazırlanmasında önerilen modele dayanak teşkil eden bilgiler betimsel araştırma modeli ile literatür taranarak derlenmiş, elde edilen bilgiler ise analitik gözden geçirme ve sistematik haritalama ile analiz edilerek sınıflandırılmıştır. Literatürde yer alan bilgiler dışında modelin kullanılması için gerekli olan dış veri, hazırlanmış olan standart bilgi toplama formu ile temin edilmiş, temin edilen veri, analizler sonucunda oluşturularak sınıflandırılmış olan bilgiler ile birlikte değerlendirilerek yorumlanmıştır. Çalışmanın yöntemi ve kullanılan araştırma tekniklerine ilişkin gösterim Şekil 3.1'de verilmiştir.



Şekil 3.1. Çalışmanın yöntemi ve kullanılan araştırma teknikleri

Tezin İkinci Bölümünde yer verilmiş olan blokzincir teknolojisine ilişkin temel özellikler literatür taranarak alt başlıklar halinde detaylandırılmıştır. Bu bölüm aynı zamanda blokzincir teknolojisinin kullanılması kararına dayanak teşkil eden, modelin de ilk adımını oluşturan temel bilgileri içermektedir. Bu temel bilgiler içerisinde yer alan blokzincir platformlarına ilişkin literatür araştırması da İkinci Bölüm kapsamında gerçekleştirilmiştir. Blokzincir tekonolojisinin kullanılıp kullanılmaması konusundaki karardan sonra, kullanılması halinde hangi teknik özelliklere sahip bir tasarımın daha uygun olduğuna karar vermek için platform adı verilen mevcut blokzincir teknolojisi altyapıları araştırılarak en yaygın biçimde kullanılan ondört platform seçilmiştir. Çok sayıda platform içerisinden birden fazla kullanım amacına hizmet edebilen, kendi blokzincir altyapısı ve kayıt defterine sahip olan, blokzincir ekosisteminde kabul görmüş olan ve mevcut uygulama geliştirme örnekleri bulunan, açık kaynak koduna erişilebilen, geliştiricileri ve destekçileri bakımından itibarlı olarak kabul edilen, teknik dokümanları (whitepaper) bulunan platformlar tercih edilmiştir.

Yine bu bölümde, blokzincir teknolojisine ilişkin yasal düzenlemeler ve standardizasyon faaliyetleri benzer biçimde literatür taranarak detaylandırılmıştır. Standardizasyona ilişkin çalışmalar başlığı altında küresel ölçekte standart geliştirmekten sorumlu ISO ve ITU faaliyetleri ile Avrupa Birliği çalışmaları derlenmiş, devletler tarafından yürütülen düzenleme faaliyetlerinde ise verilerine ulaşılabilen 66 ülke ile Avrupa Birliğince geliştirilen mevzuata dair özet bilgiler sunulmuştur. Türkiye'de blokzincir ile ilgili olduğu değerlendirilen mevzuat çalışmaları ise ayrı bir başlık halinde verilmiştir.

Literatür tarama ile hazırlanmış olan bir diğer alt başlık uluslararası kuruluşlar ve devletlerce yürütülen çalışmalara ilişkindir. Bu kısımda araştırma yapılırken, tüm dünya devletleri araştırma evreni olarak kabul edilmekle birlikte, veri erişimi kısıtlılıkları ve ülkemizin Birleşmiş Milletler e-Devlet Gelişim İndeksi sıralaması dikkate alınarak, öncelikli olarak Türkiye'nin üzerinde bulunan ülkelere odaklanılmıştır. Buna göre, dünya devletlerinde blokzincir teknolojisinin mevcut kullanım durumu konusunda araştırma evreni 193, bunlardan seçilen örneklem sayısı 60, verilerine ulaşılabilen örneklerin sayısı da 53 olarak gerçekleşmiştir. Bu literatür taraması ile, devletler ve bazı uluslararası kuruluşlar tarafından gerçekleştirilen gerçek dünya uygulamaları ile teorik çalışmalar derlenerek blokzincirin kullanım alanları çıkarılmıştır.

Literatür tarama ile son olarak blokzincir teknolojisinin uygulanabilir olup olmadığına ilişkin karar ağaçlarına ve Çok Kriterli Karar Verme yöntemlerine yönelik araştırma yürütülmüştür. En uygun metodun belirlenmesi için yedi Çok Kriterli Karar Verme metodu seçilmiş, bunlardan her biri açıklanarak beşi örnek bir senaryo üzerinden değerlendirilmiş, aynı senaryo için sayısal işlemler gerçekleştirilerek birbirleri ile karşılaştırılmıştır. Çok Kriterli Karar Verme sürecinde ağırlıklandırma metodunun seçiminde literatür tarama yolu ile çalışma konusuna benzer problemlerin çözümünde en sık kullanılan yaklaşımlar araştırılarak en uygun çözüm olarak Analitik Hiyerarşi Prosesi (AHP) seçilmiştir.

Her bir alternatifin (platform) değerlendirilmesi için beş ana başlık (teknik, performans, güvenlik, kullanım amacı ve nitel) altında toplam 23 kriter belirlenmiş, bu kriterlere göre daha sonra platform eklenmesi halinde doldurulmak üzere tüm ilgili kriterlerin detaylı açıklamalarını içeren bir şablon hazırlanmıştır (Bkz. Çizelge 2.6). Hazırlanmış olan şablon seçilen 14 platform için doldurulmuştur. Her bir platformun birbirleri ile kıyaslanması için kullanılacak kriterlere ilişkin veriler bu form vasıtası ile, her bir platformun resmi web sitesi, teknik dokümanı, github platformunda yayınlanmış olan kaynaklar ve literatür bilgileri taranarak toplanmıştır. Bu kriterler önerilecek blokzincir çözümüne en uygun platform alternatifinin değerlendirilmesi için kullanılmaktadır. Değerlendirmenin yapılabilmesi için 14 platform alternatifinin özellikleri bir arada değerlendirilmiş, birbirleri ile karşılaştırma yapılabilecek biçimde sayısal özellikler "var", yok", "çok düşük - çok yüksek" aralığı ya da "düşük - yüksek" aralığında standart dilsel değişkenlere dönüştürülerek platform karşılaştırma tablosu (Bkz. Çizelge 4.7) oluşturulmuştur.

Literatür tarama ile derlenen bilgiler daha sonra modelde kullanılmak üzere analiz edilerek listeler, karşılaştırma tabloları, karar ağacı ve kurallar oluşturulmuştur. Bu analizler ve çıktıları aşağıdaki biçimdedir:

- Dünyada kamu uygulamalarından kullanım örnekleri sistematik literatür tarama ve sistematik haritalama çalışması yapılarak sınıflandırılmıştır. Petersen, Vakkalanka ve Kuzniarz (2015) tarafından tanımlanmış olan sistematik haritalama belirli bir araştırma alanına yönelik olarak belirlenmiş olan sınıflandırma ve kategorilere ilişkin literatürün sistematik bir biçimde analiz edilmesine ve belirlenmiş olan araştırma soruları doğrultusunda sonuç çıkarma işlemidir. Bu metotlarla toplanan bu örnekler, uygulamanın konusu, kullanım motivasyonu (gerekçe ve kök neden), uygulamanın sınıfı (pilot çalışma, araştırma, model önerisi, uygulama örneği, program tasarımı vb.),

uygulama örneği ile teknik özellikleri (blokzincir platformu, yazılım dili, mutabakat mekanizması vb.) gibi bilgileri içerecek biçimde listelenerek blokzincirin kullanım durumuna ilişkin genel karakteristikler çıkarılmıştır.

- Aynı biçimde, seçilen sürecin hâlihazırda uygulaması bulunan bir süreç olup olmadığı, gerçek dünya kamu hizmet uygulamalarında denenip denenmediğini tespit ederek teknolojinin ilk aşamada kullanılabilirlik durumunu test etmek üzere dünya devletleri ve bazı uluslararası kuruluşlarca yürütülen çalışmalar da sistematik biçimde incelenmiştir.
- Çıkarılan özellikler blokzincirin kullanım kararının verilmesinde faydalanılmak üzere düzenlenmiş, blokzincirin temel özellikleri, avantajları ve kısıtlılıkları dikkate alınarak ne zaman ve hangi durumda kullanılabilir olduğu, hangi durumlarda kullanılmasının uygun olmadığı bilgilerine göre seçilen herhangi bir sürecin ilk aşamada değerlendirmesi yapılmak üzere bir liste (Bkz. Çizelge 4.11) hazırlanmıştır.
- Literatür tarama sonucunda ortaya konulan mevcut durum daha sonra analiz edilerek blokzincir teknolojisinin temel özellikleri, avantajları ve kısıtlılıkları, potansiyel ve mevcut kullanım alanları listelenmiş, derlenen bilgiler analitik gözden geçirme ile yorumlanarak karar noktalarında kullanılmak üzere kurallar oluşturulmuştur.
- Herhangi bir sürecin blokzincir çözümüne uygunluğunu değerlendirmek için bu kurallar doğrultusunda 12 adet soru belirlenmiştir (Bkz. Çizelge 4.1). Bu sorular kullanılarak ve literatürde yer alan blokzincir teknolojisinin kullanım kararı için önerilmiş olan karar ağaçları analiz edilerek soruların yanıtları doğrultusunda blokzincir çözümünün uygun olup olmadığı sonucunu veren bir karar ağacı hazırlanmıştır (Bkz. Şekil 4.2).
- Blokzincir çözümüne ilişkin verilecek karar için iki temel unsur bulunmaktadır: seçim kriterleri ve çözüm alternatifleri. Seçim kriterleri süreç özellikleri ve kullanıcı tercihlerine, platform alternatifleri ise bu özellik ve tercihler ile platformların taşıdıkları özelliklerin birbirleri ile örtüşmesine bağlıdır. Nihai karar seçim kriterleri ile alternatiflerin bir arada değerlendirilmesi problemi olup çözüm için seçim kriterleri ve her bir kriterin önem derecesi belirlenmelidir. Bu kapsamda, kullanıcı ya da karar vericiden sistematik bir biçimde bilgi temini için öncelikle bir süreç bilgi toplama formu (Bkz. Ek-1) hazırlanmıştır. Hazırlanan bu form seçilen herhangi bir kamu hizmeti süreci için doldurulabilecek biçimde, jenerik sorular içermektedir. Bu form aracılığı ile alınan bilgilerden sürecin mevcut durumunun çıkarılması, süreçte rol alan tarafların ve rollerinin belirlenmesi, sürecin blokzincir çözümüne göre yeniden tasarlanması ve seçime esas kriterlerin önceliklerinin tespitinde faydalanılmaktadır.

- Önceliklerin belirlenmesinde (kriterlerin önem derecelerinin tespitinde) 1994 yılında Oracle'da yazılım geliştirme uzmanı olarak çalışan Dai Clegg tarafından hızlı uygulama geliştirme için geliştirilmiş olan ve yazılım geliştirme, proje yönetimi gibi birçok alanda uygulanabilen bir önceliklendirme tekniği olan MoSCoW metodu kullanılmaktadır. Metot, belirli bir amaca yönelik kriterlerin ya da özelliklerin dört sınıf altında gruplandırılmasına ve bu gruplama sonucuna göre önceliklerin derecelendirilerek alternatiflerin seçimine dayanmaktadır. MoSCoW metodu adını bu dört sınıfı ifade eden "Must have (M)", "Should have (S)" "could have (C)" ve "will not have (W)" terimlerinden almaktadır. Bu sınıflandırmaya göre, belirlenmiş olan özellik ya da niteliklerden karşılanması zorunlu olanlar "M", zaruri ya da hayati olmamakla birlikte önemli değer katacak olanlar "S", bulunması iyi olan, bulunmaması halinde çıktıya etkisi küçük olanlar "C" ve bulunması istenmeyenler de "W" ile ifade edilmektedir. Model önerisinde, blokzincir teknolojisinin uygulanacağı sürece ilişkin olarak, belirlenmiş olan 17 nitelik için MoSCoW seçimi yapılmakta (Bkz. Çizelge 4.18), bu seçimlere dayanarak kullanıcı öncelikleri belirlenmektedir. Kullanıcı önceliklerinin tespiti ve analizi için kullanılan MoSCoW metodu veri girişine izin veren, kullanıcıya altı ana başlık altında 17 niteliğe ilişkin "olması gereken", "olması faydalı olan", "olması iyi karşılanan" ve "olmaması gereken" seçeneklerini içeren bir form olarak tasarlanmıştır. Belirlenen kullanıcı öncelikleri daha sonra AHP hesaplamalarında, niteliklerin ve alternatiflerin ikili karşılaştırmalarındaki matris değerlerinin belirlenmesinde kullanılmaktadır. MoSCoW nitelik listesi ile alınan kullanıcı tercihlerinin AHP'ye uyarlanmasında AHP için temel ölçek (Bkz. Çizelge 2.41) kullanılmaktadır.
- Kullanıcı veri girişleri sadece MoSCoW ile sınırlı değildir. Bu listedeki özellikler dışında "çok düşük", "çok yüksek" gibi dilsel değişkenler içeren tercihler de bulunmaktadır. Bu tercihlere ilişkin yedi nitelik de Analitik Hiyerarşi Prosesinde ikili karşılaştırmalarda kullanılmak üzere bir liste olarak hazırlanmıştır.
- Alternatifler (platform) ve kriterlerin belirlenmesinden sonra, seçilen kriterlere en uygun alternatiflerin sıralanması için Çok Kriterli Karar Verme Metodu kullanılmaktadır. Kriter ve alternatif sayısının fazla olması AHP ikili karşılaştırma matris işlem sayısını üstel olarak artırmakta ve karmaşıklaştırmaktadır. Bu nedenle, kriter ve alternatif sayısı belirlendikten sonra, ilk olarak vazgeçilmez özelliklere göre alternatifler içerisinden eleme yapılmakta, daha sonra kalan kriterler ve alternatifler için AHP uygulanmaktadır. Vazgeçilmez özelliklerin az sayıda olması ve bu nedenle alternatiflerin ve kriterlerin

sayısının ilk eleme sonucunda azaltılamadığı durumlarda Ağırlıklandırılmış Toplam Modeli (WSM) gibi metotların kullanılması önerilmiştir.

Bilgi toplama, analiz etme ve kuralları oluşturma işlemlerinden sonraki aşama süreç seçimi, sürece ilişkin bilgilerin toplanması ve hazırlanmış olan soru ve bilgi edinme formlarına veri girişidir. Kullancı(lar) ya da karar verici(ler) tarafından Ek-1'de verilmiş olan süreç bilgi formu ve Çizelge 4.18 MoSCoW özellik listesine verilen cevaplar ile modele dış bilgi girişi sağlanmaktadır. Alınan bu bilgiler sürecin hem mevcut durumuna hem de istenen durumuna ilişkin unsurlar ile kullanıcı ya da karar vericinin öncelikleri ve tercihlerini içermektedir. Bu bilgilerin bir kısmı blokzincirin uygulanabilir bir çözüm olup olmadığı kararının verilmesinde, bir kısmı da blokzincir platform alternatiflerinin belirlenen kriterlere göre en uygundan en az uygun olana doğru sıralanmasında faydalanılmaktadır. Ayrıca, edinilen bilgiler, blokzincir platform alternatifleri sıralandıktan sonra sürecin blokzincir çözümüne uygun biçimde tasarlanmasında, bu tasarımdaki rollerin ve önerilen blok yapısının belirlenmesinde faydalanılmaktadır.

Bu tez çalışması kapsamında önerilen model özetle karmaşık bir karar verme sürecinin sistematik ve iyileştirilebilir-geliştirilebilir bir biçimde tasarımına dayanmaktadır. Model geliştirilirken öncelikle araştırma soruları belirlenmiş, literatür tarama ve bilgi edinme bu sorular doğrultusunda gerçekleştirilmiştir. Bu araştırma soruları:

- Blokzincir teknolojisinin temel özelliklerinin, güçlü yönlerinin, sunduğu fırsatların, zayıf yönleri ve kısıtlılıklarının neler olduğu,
- Bu özelliklerin blokzincirin seçilen bir süreç için uygun çözüm olup olmadığı kararını vermek için nasıl kullanılabileceği,
- Uygun blokzincir çözümü kararı için hangi kriterlerin dikkate alınacağı,
- Hangi blokzincir çözüm alternatiflerinin mevcut olduğu ve bu alternatiflerin özelliklerinin belirlenen seçim kriterlerine göre nasıl sınıflandırılabileceği,
- Çok sayıda kriter ve alternatif bulunması durumunda kullanılabilecek karar verme metotlarının neler olduğu konularını kapsamaktadır.

Bu sorulara yanıt verecek biçimde modelin geliştirilmesinde izlenen yöntem de karar verme sürecine benzer biçimde birbirini takip eden adımlar halinde, aşağıdaki aşamaları içermektedir:

- Araştırma soruları ve karar konularının belirlenmesi,
- Bilgi toplama, analiz ve toplanan bilgilerin sınıflandırılması,
- Karar noktalarında kullanılacak yöntemlerin belirlenmesi,
- Toplanan bilgilerin standart formlar ve şablonlar kullanılarak işlenebilir hale getirilmesi,
- Seçilen yöntemlere ve toplanan bilgilere göre kuralların oluşturulması,
- Oluşturulan kurallara göre yapılacak değerlendirme ve hesaplamaların belirlenmesi,
- Değerlendirme ve hesaplama sonuçlarının sunumu.

Modelin geliştirilme süreci aynı zamanda model işlem adımlarını da oluşturmaktadır. Önerilen model "Bilgi Tabanı", "Kural Tabanı", "Süreç Seçimi, Bilgi Toplama ve Veri Girişi", "Hesaplama Motoru", "Teknoloji Seçimi ve Sistem Tasarımı" olmak üzere beş adımdan oluşmaktadır.

Hazırlanmış olan kural listeleri, karar ağacı ve Çok Kriterli Karar Verme metodu işlem adımları süreç analizi ve kullanıcıdan alınan tercih ve öncelikler ile birlikte, hesaplama işlemlerinin gerçekleştirildiği adımda kullanılmaktadır. Hesaplama adımında öncelikle Boolean karar ağacı yapısı kullanılarak kesinlikle evet ve kesinlikle hayır olarak cevaplanabilen sorular doğrultusunda blokzincir teknolojisinin kesinlikle uygun olmadığı durumlar değerlendirilmektedir. Boolean karar ağacı kullanılarak blokzincirin kullanılabileceği sonucuna ulaşılması halinde bir sonraki aşamada daha önceki adımda hazırlanmış olan daha detaylı karar ağacı kullanılarak blokzincirin uygun çözüm olup olmadığı değerlendirilmektedir. Blokzincirin uygun çözüm olduğu ya da önerilmemekle birlikte kullanımında sakınca olmadığı sonucuna ulaşılması halinde Analitik Hiyerarşi Prosesi işlem adımları ile gerekli detaylı hesaplamalar gerçekleştirilmekte, hesaplama sonucuna göre blokzincir platform alternatifleri öncelik sırasına alınmaktadır.

Hesaplama işlemleri tamamlandıktan sonra, sonuçlar daha önceki adımlarda derlenen, kullanıcıdan alınan ve analiz edilen bilgiler ile konsolide edilerek sistemin tasarımı oluşturulmaktadır. Modelin hesaplama işlemlerini takip eden adımında analitik gözden geçirme yöntemi ile değerlendirilen çıktılar sürece ilişkin yeni iş akış şeması, değerlendirme notları ve sistemin teknik özelliklerinin bir listesi biçiminde sunulmaktadır.

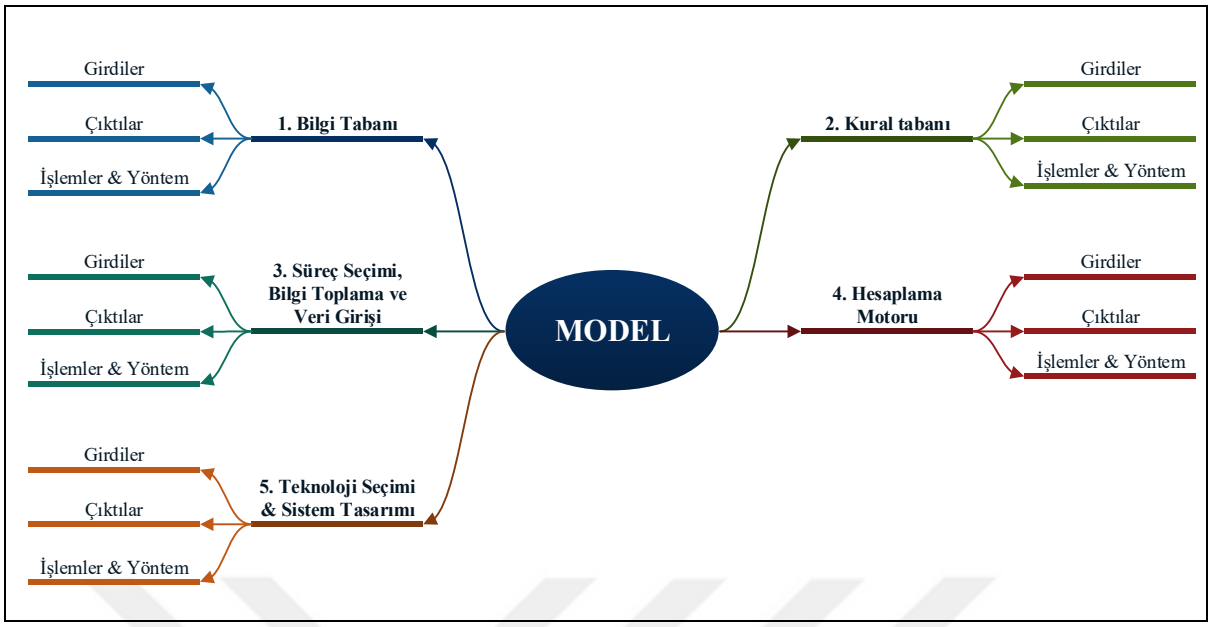
4. BLOKZİNCİR TEKNOLOJİSİNİN KULLANIMI İÇİN BİR MODEL ÖNERİSİ

Bu tez kapsamında önerilen model ile blokzincir teknolojisinin mevcut bir kamu hizmeti süreci için uygulanabilir olup olmadığının tespit edilmesi, uygulanabilir bulunması halinde sistemin özellikleri ve tasarımının ortaya konulması hedeflenmektedir.

Blokzincir teknolojisinin kullanım kararına ilişkin olarak önerilen model temel olarak genel niteliklerin derlenerek kuralların oluşturulması, blokzincirin uygulanacağı sürece ilişkin bilgilerin toplanması, belirlenen kurallara göre blokzincirin uygun çözüm olup olmadığına, uygun çözüm olması halinde nasıl bir tasarıma sahip olması gerektiğine karar verilmesini içermektedir.

Bu kapsamda, öncelikle, tezin ikinci bölümünde yer verilmiş olan bilgiler ışığında blokzincir teknolojisine ilişkin nitelikler ve temel kurallar belirlenmektedir. Daha sonra blokzincir çözümünün uygulanacağı sürece ilişkin bilgiler toplanarak birinci aşamada oluşturulan kurallara göre değerlendirilebilecek biçimde sınıflandırılmaktadır. Bu sınıflandırmadan sonra, belirlenmiş olan karar noktalarına göre süreç nitelikleri ile blokzincir nitelikleri ve kurallar kıyaslanarak uygun seçim alternatifleri belirlenmekte, bunlardan her biri belirlenmiş olan seçim kriterlerine göre puanlanarak önem derecelerine göre sıralanmaktadır.

Buna göre, blokzincir teknolojisinin kamu hizmetlerinde kullanımı için önerilen model beş temel adım olarak tasarlanmıştır. Bu temel adımlar Şekil 4.1'de verilmiş olup her bir adım için girdiler, işlemler ve çıktılar olmak üzere üç alt başlık belirlenmiştir.



Şekil 4.1. Model işlem adımları

4.1. Model İşlem Adımları

Kamu hizmetlerinde blokzincir teknolojisinin uygulanmasına ilişkin olarak önerilen modelin ana ve alt adımları aşağıdaki biçimdedir:

4.1.1. Adım 1. Bilgi Tabanı

Modelin yapılandırılması ve karar noktaları için kuralların oluşturulmasında kullanılacak olan bilgilerin derlendiği adımdır. Bu adımda blokzincir teknolojisinin özellikleri belirlenerek avantajlı ve dezavantajlı olduğu konular sınıflandırılmakta, dünyadan kullanım örnekleri analiz edilerek en uygun olduğu alanların ortak özellikleri derlenmekte, karar noktaları belirlenerek bu karar noktaları için gerekli bilgi ve yöntemlerin çıkarılması sonucunda ikinci adıma girdi teşkil edecek çıktılar liste, tablo ve karar ağacı biçiminde üretilmektedir.

Modelin bu adımı ağırlıklı olarak blokzincir teknolojisi hakkında literatür tarama ile elde edilen bilgilerin sınıflandırılması ve analizine dayanmaktadır. Bu adımdaki bilgiler genel literatüre, temel özellik ve mevcut durum bilgilerine dayandığından kısa vadede radikal biçimde bir güncellenme gereksinimi öngörülmemektedir. Bununla birlikte, adımın

çıktılarında yer alan liste, tablo ve metotlara yapılacak ilave, çıkarma ya da değişikliklerin modelin işleyişine etkisi bulunmamaktadır.

Bilgi tabanı adımının girdileri, bu adımda gerçekleştirilen işlemler ve bu işlemler sonucunda elde edilen çıktılar aşağıdaki biçimdedir.

Girdiler

Modelin ilk adımı için kullanılan bilgiler bu çalışmanın ikinci bölümünde yer verilmiş olan aşağıdaki konuları içermektedir:

a) Blokzincir teknolojisinin temel özellikleri
   - Blokzincirin güçlü yönleri ve sunduğu fırsatlar (Bölüm 2.1.6)
   - Blokzincirin zayıf yönleri ve kısıtlılıklar (Bölüm 2.1.7)
   - Potansiyel kullanım alanları (Bölüm 2.1.5)
   - Mevcut kamu uygulamaları (Bölüm 2.3)
   - Blokzincir platformlarının özellikleri (Bölüm 2.1.12)
b) Blokzincir kullanımı karar modelleri (Bölüm 2.6)
c) Çok Kriterli Karar Verme Metotları (Bölüm 2.7)

İşlemler

İlk adımda girdi olarak sayılanlar üzerinde gerçekleştirilen işlemler sırasıyla aşağıdaki biçimdedir:

Araştırma soru ve konularının belirlenmesi

Bu kısımda, modelin sonraki adımlarında kullanılmak üzere, yanıtlarından karar noktalarında faydalanılan sorular ve bu soruların yanıtları derlenmektedir. Bu işlem, ilk adımın takip eden diğer işlem ve faaliyetlerinin de kapsamının belirlendiği işlemdir. Temel model için araştırma soru ve konuları aşağıdaki biçimdedir:

- Blokzincir ne zaman kullanılmalıdır?
- Blokzincir ne zaman kullanılmamalıdır?
- Blokzincirin sağladığı avantajlar ve güçlü yönleri nelerdir?

- Blokzincirin kısıtlılıkları ve dezavantajlı olduğu konular nelerdir?
- Blokzincir teknolojisinin hâlihazırda kullanıldığı alanlar nelerdir?
- Blokzincir teknolojisinin kullanılabileceği alanlar nelerdir?

Literatür araştırması ile teknolojinin araştırma soruları ve konu başlıkları kapsamında anlaşılması

Bu kısımda, genel literatür araştırması ile blokzincir teknolojisinin temel özellikleri, çözüm getirdiği sorunlar ve teknik özellikleri çıkarılmakta, teknolojinin anlaşılması ve bu bilgilerin karar noktalarında kullanılması için listelenmektedir. Tezin ikinci bölümü bu işlevi görmektedir.

Toplanan bilgilerin analiz edilmesi ve sınıflandırılması

Önceki kısımda yapılan araştırmanın sonuçları konsolide edilerek ilk kısımdaki sorulara cevap verecek biçimde listelenmek üzere analiz edilmektedir. Bu analiz sonucunda aşağıdaki işlemler gerçekleştirilmektedir:

- Temel özelliklerin listelenmesi,
- Avantaj ve güçlü yönlerin listelenmesi,
- Kısıtlılıklar ve dezavantajların listelenmesi,
- Potansiyel kullanım alanlarının listelenmesi,
- Mevcut uygulamaların listelenmesi,

Blokzincir teknolojisi kullanımı kararı için karar ağaçlarının analiz edilerek yeni bir karar ağacı yapısının oluşturulması

Blokzincire ihtiyaç olup olmadığının tespit edilmesi için blokzincir teknolojisinin temel özellikleri ve alternatiflerine göre güçlü ve zayıf yanları iyi analiz edilmelidir. Teknolojinin uygulanmaya başlanmasından önce verilmesi gereken bu kritik karar için karar vericiler yeterli teknik bilgiye sahip olmayabilir. Bu nedenle bu ilk karar noktası için temel bazı soruları içeren çeşitli karar ağaçları geliştirilmiş, literatürde yer alan bu çalışmalara İkinci Bölümde yer verilmiştir.

Geliştirilmiş olan bu karar ağaçları incelenmiş, İkinci Bölümde detaylı biçimde açıklanan blokzincir özellikleri de dikkate alınarak blokzincirin seçilen konu ya da iş süreci için uygun çözüm olup olmadığı konusunda verilecek karara destek olmak üzere yeni bir karar ağacı oluşturulmasına karar verilmiştir. Bu karar ağacı oluşturulurken öncelikle karar için gerekli sorular derlenmiş, bu sorular öncelikle iki grupta toplanmıştır:

1. Blokzincir çözümünün uygun olup olmadığına kesinlikle "evet" ve "hayır" cevabı verilebilen sorular,
2. Blokzincir seçiminin uygun olması halinde blokzincir tipinin (açık, gizli, izin gerektiren, izin gerektirmeyen gibi) seçimine yönelik sorular.

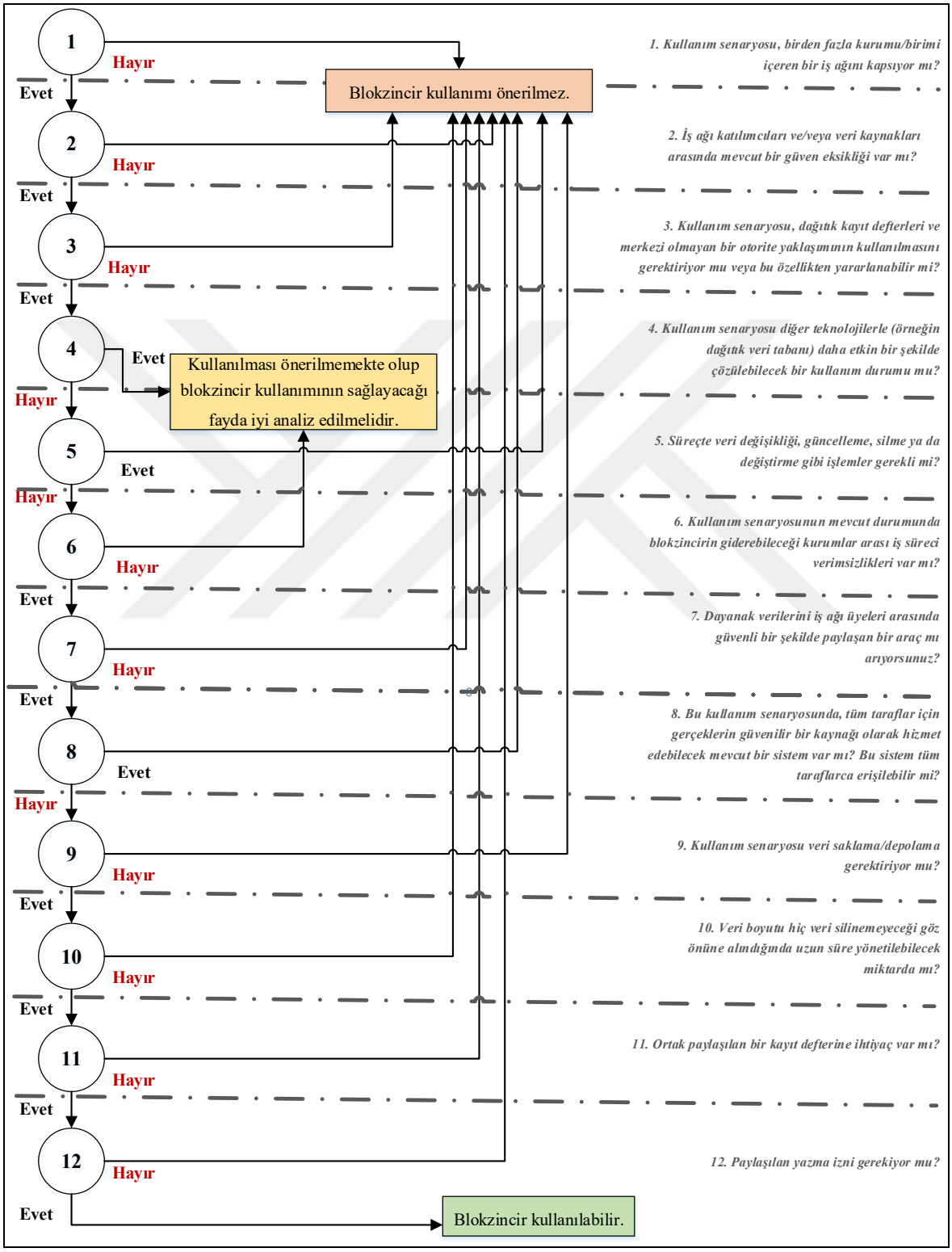
Bu sorular belirlendikten sonra öncelik sırasına alınarak sorunun cevabının "evet" ya da "hayır" olmasına göre izlenecek adımlar listelenmiş, daha sonra bu liste kullanılarak akış şeması hazırlanmıştır. Bu sorular ve ilgili açıklamalar aşağıda, Çizelge 4.1'de verilmiştir.

Çizelge 4.1. Kullanım senaryosu için blokzincir çözümünün uygun olup olmadığı kararında kullanılan sorular

	Soru	Açıklama	Evet	Hayır
1	Kullanım senaryosu, birden fazla kurumu/birimi içeren bir iş ağını kapsıyor mı?	*Tek bir kurum/birimin yönetiminde olan kullanım senaryosu kavram kanıtlama ya da pilot çalışma için kullanılabilir ancak birden fazla kurum/kuruluşun dâhil olduğu senaryolar blokzincir için daha uygundur. Bu kuruluşlar blokzincir kullanarak ortak bir varlık paylaşmaya ya da fikir birliği gerektirmeye çalışacaktır.*	Blokzincir kullanılabilir.	Blokzincir kullanımı önerilmez.
2	İş ağı katılımcıları ve/veya veri kaynakları arasında mevcut bir güven eksikliği var mı?	*Blokzincirin veri bütünlüğünü desteklediği ancak veri kalitesini doğrulamak için doğal yetenekleri olmadığı unutulmamalıdır. Kaynaklar arasında Nesnelerin İnterneti (IoT) cihazları, eski sistemler, servis sağlayıcılar ve birden fazla kurumdaki kullanıcılar olabilir. Güven eksikliği ifadesinden tarafların birbirleri hakkında kısıtlı bilgiye sahip olmaları ve birbirlerini denetleyememeleri anlaşılmalıdır.*	Blokzincir kullanılabilir.	Blokzincir kullanımı önerilmez.
3	Kullanım senaryosu, dağıtık kayıt defterleri ve merkezi olmayan bir otorite yaklaşımının kullanılmasını gerektiriyor mu veya bu özellikten yararlanabilir mi?	*Kullanım senaryosu tek bir merkezin yönettiği yapıdan vazgeçilerek dağıtık mutabakat yapısının kullanılmasına uygun mu? Sürecin dağıtık kayıt defteri ve merkezi olmayan otorite yaklaşımı ile yeniden tasarlanması işlemlerin daha hızlı, daha güvenilir ve etkin biçimde gerçekleşmesini sağlayabilir mi?*	Blokzincir kullanılabilir.	Blokzincir kullanımı önerilmez.
4	Kullanım senaryosu diğer teknolojilerle (örneğin dağıtık veri tabanı) daha etkin bir şekilde çözülebilecek bir kullanım durumu mu?	*Bu teknolojiler bir blokzincir çözümünün bu kullanım durumu için sağlayacağı faydaları sağlıyor mu ve bu çözüm tüm taraflar için uygulanabilir mi?* *Kullanım senaryosunda sadece blokzincirin sunduğu özelliklerden (örneğin verilerin silinememesi, değiştirilememesi gibi) faydalanılması gerekiyor mu?* *Örneğin, çok miktarda kritik bilgi içeren (sağlık verileri gibi), çok sayıda paydaşın dâhil olduğu kullanım durumlarında dağıtık veri tabanı verimli ve ekonomik olmayabilir.*	Kullanılması önerilmemekte olup blokzincir kullanımının sağlayacağı fayda iyi analiz edilmelidir.	Blokzincir kullanılabilir.
5	Süreçte veri değişikliği, güncelleme, silme ya da değiştirme gibi işlemler gerekli mi?	*Blokzincirde işlem girişleri sadece ekleme içindir. İşlem kayıtları değiştirilemez ve silinemez (yönetici tarafından bile). Kullanım durumu katı biçimde işlem değişmezliği gerektiriyor veya bu özellikten yararlanabilir ise blokzincir kullanılabilir.*	Blokzincir kullanılamaz	Blokzincir kullanılabilir.
6	Kullanım senaryosunun mevcut durumunda kurumlar arası iş süreci verimsizlikleri var mı? Blokzincirin kendisine has özellikleri bu verimsizlikleri giderebilir mi?	*Kurumlar arasında bilgi doğrulama için çok uzun zaman geçmesi, süreci uzatan ve maliyeti artıran bürokrasi gibi sorunlar ve iyileştirilebilir alanlar var mı?*	Blokzincir kullanılabilir.	Kullanılması önerilmemekle birlikte blokzincir kullanımının sağlayacağı fayda iyi analiz edilmelidir.

	Soru	Açıklama	Evet	Hayır
7	Dayanak verilerinin iş ağı üyeleri arasında güvenli bir şekilde paylaşıldığı bir araç mı aranıyor?	*Kullanım senaryosu birden fazla taraf arasında güvenli bir biçimde paylaşılan verileri, bu verilere ilişkin doğrulama ve onay mekanizmalarının mutabakatla gerçekleşmesini gerektiriyor mu?*	Blokzincir kullanılabilir.	Blokzincir kullanımı önerilmez.
8	Bu kullanım senaryosunda, tüm taraflar için gerçeklerin güvenilir bir kaynağı olarak hizmet edebilecek mevcut bir sistem var mı? Bu sistem tüm taraflarca erişilebilir mi? (Sürekli çevrimiçi güvenilir bir üçüncü taraf kullanılıyor mu?)	*Güvenilir ve erişilebilir bir merkezi bir otorite tarafından sağlanan kayıtların bulunması halinde blokzincir çözümüne gerek duyulmayabilir. Bu merkezi otorite ya da aracının güvenilir olması, ek maliyet getirmemesi ya da getirdiği maliyetin yapılacak yatırımdan daha düşük olması gibi durumlarda blokzincir çözümünün getireceği fayda detaylı biçimde analiz edilmelidir. (Örneğin, dijital sürücü belgesinin verilmesi sürecinde basılı kâğıt ortamında başvuru evrakları, eğitim devam çizelgeleri, sınav sonuçları güvenilir veri kaynağı olarak tutulmakta ve sunulmaktadır. Tüm taraflar bu verilere açık biçimde ulaşamamaktadır. Süreç içerisindeki her bir otorite kendi verisini tutmaktadır.)*	Blokzincir kullanımı önerilmez.	Blokzincir kullanılabilir.
9	Kullanım senaryosu veri saklama/depolama gerektiriyor mu?	*Blokzincir temelde silinemeyen, değiştirilemeyen kayıtları içeren bir kayıt defteridir. Kullanım senaryosu bir veri saklama ve depolama işlevi gerektirmiyorsa blokzincirin kullanılması uygun olmayabilir.*	Blokzincir kullanılabilir.	Blokzincir kullanımı önerilmez.
10	Veri boyutu hiç veri silinemeyeceği göz önüne alındığında uzun süre yönetilebilecek miktarda mı?	*Büyük hacimli veri saklamaya uygun az sayıda blokzincir platformu olmakla biirlikte, blokzincir teknolojisinin genel olarak yüksek hacimli veriler için uygun bir çözüm olmadığı unutulmamalıdır. Büyük hacimli verilerle ilgili blokzincir uygulamalarında BigchainDB gibi platformlar ya da zincir dışı depolama çözümleri kullanılabilmektedir.*	Blokzincir kullanılabilir.	Blokzincir kullanımı önerilmez.
11	Ortak paylaşılan bir kayıt defterine ihtiyaç var mı?	*Blokzincir teknolojisinde tutulan kayıtlar tüm ağ düğümlerinde özdeş biçimde tutulmaktadır. Ağ üyelerinin her birinin güncel kayıt defterini kendisine tutması gerekiyorsa blokzincir uygun bir çözümdür.*	Blokzincir kullanılabilir.	Blokzincir kullanımı önerilmez.
12	Paylaşılan yazma izni gerekiyor mu?	*Blokzincir teknolojisinde işlem gerçekleştirme talebi gönderildikten sonra o işlemin uygunluğunun kontrolü, onayı ve kaydın gerçekleşmesi fikir birliği mekanizmaları kullanılarak sağlanır. Paylaşılan yazma izni ile kastedilen ağda izin verilen tüm tarafların işlem talebinde bulunması, bu taleplerin kayıt defterine kaydedilme kararının ise tek bir otorite tarafından değil blokzincir ağı tarafından verilmesidir.*	Blokzincir kullanılabilir.	Blokzincir kullanımı önerilmez.

Çizelge 4.1'de verilmiş olan sorular kullanılarak hazırlanmış olan karar akış şeması Şekil 4.2'de verilmiştir.



Şekil 4.2. Kullanım senaryosuna göre blokzincir kullanımı için karar akış şeması

Çizelge 4.1'de verilmiş olan sorular kullanılarak kullanım senaryosu değerlendirildikten sonra blokzincir çözümünün kullanılabilir olması sonucuna ulaşılması halinde, blokzincir tipinin nasıl olacağına karar verilmektedir. Buna göre;

- Kayıt defterini herkesin kullanması isteniyorsa, herkes blokzincir ağına katılabiliyorsa "Açık Blokzincir"
    - Kayıt defterinin doğruluğunu sağlamak için ödül-teşvik sistem içindeyse, ağa katılan herkes mutabakat sistemine dâhil olabiliyorsa "Bütünüyle izin gerektirmeyen açık blokzincir",
    - Kayıt defterinin doğruluğunu sağlamak için ödül-teşvik sistem dışındaysa, ağa katılan herkes mutabakat sistemine dâhil olamıyorsa "Kısmen izin gerektirmeyen açık blokzincir",
- Kayıt defterini sadece belirli bir grup kullanacaksa, blokzincir ağına katılım izne tabiyse "Özel Blokzincir"
    - Kayıt defteri doğruluğunu tüm grup üyeleri sağlıyorsa, ağa katılan herkes mutabakat sistemine dâhil olabiliyorsa "İzin gerektiren özel blokzincir",
    - Kayıt defteri doğruluğunu ayrıcalıklı grup üyeleri sağlıyorsa, ağa katılan herkes mutabakat sistemine dâhil olamıyorsa "Bütünüyle izin gerektiren özel blokzincir" olarak adlandırılan tasarım kullanılmalıdır.

Bu kısımda oluşturulmuş olan karar ağacı birinci aşama karar için kullanılmakta olup blokzincir teknolojisinin özelliklerinde gelecekte meydana gelecek değişiklikler doğrultusunda güncellenebilecektir.

Çok Kriterli Karar Verme Metotlarının incelenerek en uygun metodun seçilmesi.

İlk adımın bu kısmında blokzincir çözümü alternatiflerinin farklı kriterlere göre birbirleri ile kıyaslanarak sıralanması bir Çok Kriterli Karar Verme problemi olarak ele alınmış, bu problemin çözümü için kullanılabilecek metotlar araştırılmıştır. Bölüm 2.7'de detayları verilmiş olan bu metotlar içerisinden öncelikle Analitik Hiyerarşi Prosesinin kullanılmasına karar verilmiştir. Seçilen sürece ilişkin kriterlerin ve alternatiflerin sayıları, sürecin özellikleri ve Çok Kriterli Karar Verme metotlarında meydana gelebilecek değişiklikler dikkate alınarak herhangi bir metodun kullanımına karar verilebilecektir.

Çıktılar

Modelin sonraki aşamalarında kullanılmak üzere bu adımda elde edilmiş olan çıktılar aşağıdaki biçimdedir:

Temel özelliklere ilişkin listeler

Temel özellikler blokzincir teknolojisinin kullanımı ile ilgili karar verilirken dikkate alınacak olan, fonksiyonel ve fonksiyonel olmayan gereksinimleri içermektedir. Fonksiyonel olan gereksinimler teknolojiyi veri tabanları gibi diğer teknolojilerden ayıran, mevcut problemlere çözüm getirebilecek olan, işleyişi doğrudan etkileyen özellikleri, fonksiyonel olmayan gereksinimler ise işleyişi doğrudan etkilememekle birlikte verimlilik ve performans gibi seçim kararında önemli yeri olan kriterleri içermektedir. Bu özellikler karar ağaçlarında, seçim kararına ilişkin hesaplamalarda kullanılan kriterlerin belirlenmesinde ve sürece ilişkin bilgi edinilmesinde kullanılmaktadır. Buna göre, bu özellikler aşağıdaki Çizelge 4.2 ve 4.3'te verilmiştir.

Çizelge 4.2. Blokzincir teknolojisinin kullanımının uygun olduğu ve olmadığı durumlar

Ne zaman blokzincir kullanılmalı?	**Ne zaman blokzincir kullanılmamalı?**
• Birden fazla taraf arasında veri paylaşımı • Taraflar arasında güven eksikliği • Diğer teknolojilerle (dağıtık veritabanı gibi) etkin biçimde çözülemeyen sorunlar • Birden fazla tarafın veri girişi – güncellemesi • Veri-işlemlerin doğrulanma-onaylanma gereksinimi • Verilerin-işlemlerin değiştirilememesi-silinememesi • Veri doğrulama-onaylama için aracı (üçüncü taraf) ihtiyacının getirdiği maliyet ve karmaşıklık • İşlemlerin zamana duyarlı olması • İşlemler arasında etkileşim bulunması	• Yüksek veri hacmi • Yüksek işlem hızı • Yüksek performans (*blokzincirde performans sorunlarına çözüm getiren platformlar da bulunmaktadır*) • Geçmiş verilerde değişiklik ve/veya imha gereksiniminin bulunması • Tek bir kurumun sorumlu olduğu, merkezi olarak yönetilmesi gerekli ve verimli olan süreçler

Çizelge 4.2'te verilmiş olan özellikler, seçilen sürecin blokzincir çözümüne uygun olup olmadığını değerlendirmek için kullanılan karar ağacının oluşturulmasında kullanılmıştır.

Çizelge 4.3. Blokzincir teknolojisine ilişkin fonksiyonel ve fonksiyonel olmayan gereksinimler

Fonksiyonel Gereksinimler	Fonksiyonel Olmayan Gereksinimler
• Ortak ve tutarlı veri saklama • Birden fazla kullanıcının kayıt yazabilmesi • Tüm kayıt ekleyebilen aktörler arasında güven ve hiyerarşi eksikliği • Aracı ya da merkezi otorite bulunmaması • Kayıtların değiştirilememesi, silinememesi, güncellenememesi • Katılımcıların belirlenen düzeyde anonimliğe sahip olması	• Ölçeklenebilirlik • İşlem hızı • İşlem hacmi • Sistem güvenliği (çatallanma, mutabakat mekanizması açıkları) • Diğer sistemlerle entegrasyon • Verimlilik • Mevzuat düzenlemelerine uyum • Teknik ve süreç olgunluk/standardizasyon düzeyi • İşbirliği gereksinimi • Şeffaflık

Çizelge 4.3'te verilmiş olan fonksiyonel gereksinimler blokzincir çözümünün uygulanabilmesi için gereklilikleri, fonksiyonel olmayan gereksinimler ise işleyişi doğrudan etkilememekle birlikte performansla ilgili olan özellikleri içermektedir. Fonksiyonel gereksinimler blokzincirin uygun çözüm olup olmadığı kararında, fonksiyonel olmayan gereksinimler ise çözüm alternatiflerinin değerlendirilmesi için dikkate alınan kriterlerin belirlenmesinde kullanılmaktadır.

Avantajlar ve güçlü yönler listesi

Karar ağaçlarının oluşturulmasında ve karar ağaçlarından önce blokzincir çözümünün uygunluğunun tespitinde kullanılmak üzere teknolojinin getirdiği avantajlar ve güçlü yönleri tezin ikinci bölümünde yer verilmiş olan literatür araştırması sonuçlarına göre listelenmekte, modelin ikinci ve dördüncü adımlarında gerçekleştirilen işlemler ile, uygulanacağı süreçte bunlardan faydalanma potansiyeli değerlendirilmektedir. Buna göre, blokzincir teknolojisinin sunduğu avantajlar ve mevcut çözümlere göre güçlü yönleri Çizelge 4.4'te verilmiştir. Bu çizelgeden, sürece ilişkin analiz yapılırken "süreç bu avantajdan faydalanabilir mi?" sorusuna yanıt aranmaktadır.

Çizelge 4.4. Blokzincir teknolojisinin avantajları ve güçlü yönleri

Avantaj ve güçlü yön	Açıklama
Şeffaflık, izlenebilirlik ve denetlenebilirlik	Blokzincirde tutulan veri zaman damgası ile kronolojik olarak sıralandığından, veri yapısı dağıtık, değiştirilemez ve dışarıdan müdahaleye karşı korunaklı olduğundan bilginin kaynağı kolay izlenebilir ve güvenilir hale gelir.

Avantaj ve güçlü yön	Açıklama
Aracıların, manuel işlemlerin ve bürokrasinin fazla olduğu süreçleri sadeleştirme	Blokzincir teknoloji fikir birliği algoritmaları ile aracılar tarafından gerçekleştirilmesi gereken doğrulama ve onay işlemlerini otomatikleştirmekte, aracılara olan ihtiyacı ortadan kaldırmaktadır.
Arıza süresi sıfır olan bir sistem sunması	Dağıtık yapısı nedeniyle merkezi sistemlerdeki tek nokta hatasına karşı korumalıdır. Blokzincir ağındaki çok sayıda düğümde tutulan kayıtlar sayesinde sistemde sadece tek bir düğüm bile kalsa işleyiş devam edebilir.
Düşük işlem maliyetleri, mevcut sistemlere göre hizmetleri çok daha düşük maliyetlerle karşılama potansiyeli	Aracılardan kaynaklanan yüksek komisyon ve işlem ücretlerini düşürme potansiyelini taşımaktadır.
Eklenen verilerin silinememesi, değiştirilememesi	Blokzincir teknolojisinin tasarımı gereği kayıt defterine ilave edilen veriler silinememekte ve değiştirilememektedir. Bu durum bazı süreçler için bir avantaj iken bazıları için ise dezavantaj olabilmektedir.
Finansman sağlama kolaylıkları - İlk Dijital Para Arzı (*Initial Coin Offering - ICO*)	Kitlesel fonlama benzeri birçok finansman sağlama kolaylıkları sunmaktadır.
Güvenlik (veri şifreleme, erişim kontrolleri, kimlik yönetimi)	Kriptografinin, dijital imzaların ve hash algoritmalarının yoğun biçimde kullanıldığı, yazılıma dayalı güçlü bir güvenlik yapısı bulunmaktadır.
Hızlı ve her an (24 saat) gerçekleştirilebilir işlemler	Havale, EFT ve kredi kartı kullanımı gibi mevcut banka işlemlerine göre hız ve performans bakımından yetersiz olsa da uluslararası para transferinin, çok yüklü transferlerin çok hızlı bir biçimde ve 24 saat süresince gerçekleştirilebilmesi bir diğer avantajıdır.
Kişilerin kendi verilerinin sahibi olarak bu verilerin yönetiminde tam yetki sahibi olmaları	Tasarımı veri sahiplerinin kendi verilerini yönetebilmelerine, bilgileri istedikleri taraflarla paylaşmalarına olanak sağlamaktadır. Kişisel mahremiyet ihlal edilmeden farklı taraflar arasında veri paylaşımı mümkündür.
Mikro ve nano ödemeler olarak adlandırılan çok küçük miktarlı transfer işlemlerinin gerçekleştirilebilmesi	Mevcut bankacılık sisteminde problem yaratan çok küçük miktarlı ödeme ve transferler kolaylıkla gerçekleştirilebilmektedir.
Sosyal yardımların daha düşük maliyetle ve daha etkin biçimde dağıtılması, amaç dışı ve usulsüz kullanımının engellenmesi	Şeffaflık, izlenebilirlik ve biyometrik verilerle destekli sistemler sayesinde doğrudan ihtiyaca dönük yardımların doğru kişilere iletilmesi, düşük havale ve işlem ücretleri sosyal yardımların daha etkin biçimde dağıtılmasını sağlamaktadır.
Veri saklama, koruma ve yedekleme maliyetinin düşürülmesi	Mevcut sistemlerde verinin korunması, yedeklenmesi, iş sürekliliği ve felaket kurtarma gibi gerekliliklerin getirdiği sistem karmaşıklığı ve maliyetleri düşürme potansiyelini taşımaktadır.
Yeni gelir alanları	Başta merkeziyetsiz finans (DeFi – Decentralized Finance) olmak üzere bazı alanlarda yeni iş ve gelir alanları yaratma potansiyeline sahiptir.

Dezavantajlar ve kısıtlılıklar listesi

Avantajlar ve güçlü yönler ile benzer biçimde, karar ağaçlarının oluşturulmasında ve karar ağaçlarından önce blokzincir çözümünün uygunluğunun tespitinde kullanılmak üzere teknolojinin kısıtlılıkları listelenmekte, blokzincir çözümünün uygulanacağı süreçler bakımından bu dezavantaj ve kısıtlılıklar değerlendirilmektedir. Buna göre, blokzincir

teknolojisinin dezavantajları ve kısıtlılıkları Çizelge 4.5'te verilmiştir. Bu çizelgeden, sürece ilişkin analiz yapılırken "sürecin işleyişi bakımından bu kısıtlılık bir engel oluşturuyor mu?" sorusuna yanıt aranmaktadır.

Çizelge 4.5. Blokzincir teknolojisinin dezavantajları ve zayıf yönleri

Dezavantaj ve zayıf yön	**Açıklama**
Şeffaflık, izlenebilirlik ve denetlenebilirlik	Aynı zamanda bir avantaj olmakla birlikte, blokzincir içerisindeki kayıtların (açık blokzincir yapısında) anonim de olsa herkese açık olması kişisel veriler gibi bazı hassas ya da gizli bilgiler için istenmeyen bir durum olabilmektedir. Bu durumda, mimarinin özel blokzincir olarak tasarlanması gerekmektedir.
Eklenen verilerin silinememesi, değiştirilememesi	Hem avantaj hem de dezavantaj olarak sayılan bu özellik veri ya da kayıtlarda güncelleme, silme ya da değişiklik gereken durumlar içeren süreçlerde blokzincirin kullanımını imkânsız hale getirmektedir.
Blokzincir üçlü çelişkisi (ölçeklenebilirlik, merkezsizlik ve güvenlik)	Üzerinde çalışılmaya devam eden ve az da olsa bu soruna çözüm getirdiğini iddia eden platformlar olmakla birlikte, blokzincir mimarisi genellikle aynı anda bu üç özellikten yalnızca ikisini sağlayabilmektedir. Aynı anda güvenli, merkezsiz ve ölçeklenebilir bir sistem gerektiren süreçlerde uygulanması güçtür.
Genel veri depolamaya uygun olmama	Verilerin silinememesi nedeniyle kayıt defteri sürekli büyüyen yapıda olduğundan veri hacminin yüksek olduğu süreçler için uygun değildir. Büyük veri gerektiren uygulamalar için BigChain gibi çözümler olmakla birlikte, bu tip gereksinimi olan süreçlerde uygulanmasının gerekliliği ve etkinliği değerlendirilmelidir.
"İş İspatı" mutabakat modeli ile ilgili sorunlar (yüksek enerji tüketimi)	Bitcoin'de de kullanılan iş ispatı fikir birliği algoritması çok yüksek elektrik tüketimi gerektirmektedir.
Veri kalitesi (kaynak verisi)	Akıllı sözleşmelerin kullanımı gibi bazı durumlarda blokzincir sistemi dışından bazı güvenilir bilgilere erişilme gerekliliği dış verilerin kalitesi ve güvenilirliği konusunda bazı soru işaretleri doğurmaktadır.
Kriptografik anahtarları uygun biçimde saklama gerekliliği	Blokzincir teknolojisinin güvenliği ileri kriptografik yöntemlerle sağlanmış olmakla birlikte özellikle finansal uygulamalarda kaynağa erişim için kullanılan anahtarların saklanması sorumluluğu kullanıcılara aittir. Bu anahtarların kaybedilmesi, çalınması ya da unutulması halinde başvurulabilecek bir mercii ya da işlemleri iptal edecek ya da tersine çevirecek bir mekanizma her zaman mümkün olmamaktadır.
Ölçeklenebilirlik	Zamanla sürekli büyüyen bir ağ ya da artan işlem hacmine cevap verebilme kapasitesi güvenlik ya da merkezsizlikten fedakârlık etmeyi gerektirmektedir.
Performans	Yüksek işlem hacmi veya yüksek hız gerektiren işlemlerde mevcut merkezi veri tabanı sistemlerinin gerisindedir.
Standartların bulunmaması	Çok sayıda alternatif çözüm bulunması
Yönetişimi güç yapı	Klasik sistemlere göre farklı yapısı, tek bir merkez tarafından yönetilmemesi, kod geliştiriciler, madenciler, kullanıcılar, düğümler gibi farklı roller nedeni ile yönetişimi güçtür.
Mevzuat ve yasal düzenlemelerin yetersizliği	Mevcut Müşterini Tanı ve Kara Paranın Aklanmasının Önlenmesi düzenlemelerine uyum güçlüğü bulunmaktadır. Ayrıca, unutulma hakkı, anonimliğin korunması gibi konuları da içeren mevzuata uyuma ilişkin güçlükler bulunmaktadır.

Potansiyel kullanım alanları ve mevcut uygulamalar listesi

Blokzincir teknolojisinin ilgili sürece uygun olup olmadığı değerlendirilirken yukarıda sayılmış olan özellikler, karar ağaçları ve detaylı analizler yapmadan önce ikinci bölümde yer verilmiş olan dünyadan uygulama örnekleri ile karşılaştırma yapmak üzere potansiyel ve mevcut uygulamalar listelenmektedir. Bu listede yer alan kullanım alanlarının çoğunluğu hâlihazırda gerçek dünya uygulaması olarak kullanılmakla birlikte, literatürde kullanılabileceği alan olarak belirtilen, henüz uygulama aşamasına geçmemiş ancak üzerinde çalışılan konular da listeye ilave edilmiştir. Böylelikle, hâlihazırda test edilerek gerçek dünya uygulaması haline getirilmiş olan süreçler için bu detaylı değerlendirmelerin yapılmasına gerek duyulmamaktadır. Blokzincir teknolojisinin uygulanmış olduğu bu süreçlerin listesi Çizelge 4.6'da verilmiştir.

Çizelge 4.6. Blokzincir teknolojisinin hâlihazırda uygulanabilir olduğu süreçler

Süreç
Çok küçük miktarlı ödeme ve transferler
Dijital kimlik yönetimi
Dijital para birimi ile varlık transferi
Dijital sertifika (diploma, transkript, eğitim belgesi vb.)
Elektronik oylama
Enerji ticareti
Fon toplama, finansman ve kredi sağlama
Gayrimenkul kayıt yönetimi
Gıda ürünlerinin izlenmesi
İhale ve satınalma sistemi
İzlenebilirlik ve orijinallik kontrolü
Kişisel kayıtların yönetimi (sağlık, finans vb.)
Merkezi Olmayan Otonom Organizasyonlar (DAO)
Mesajlaşma sistemi
Noter onayı
Sadakat puanı ve ödülleri
Sosyal yardımların dağıtılması
Tedarik zinciri yönetimi
Telif hakkı yönetimi
Tokenizasyon ve sabit kripto paralar
Uluslararası para transferi
Varlık Kaydı ve Yönetimi
Veri toplama, kayıt ve paylaşımı

Platform karşılaştırma tablosu

İkinci Bölümde detaylı biçimde yer verildiği üzere, standart, tek bir blokzincir mimarisi bulunmamaktadır. Her biri farklı yapıya sahip, farklı sorun ve çözümlere odaklanmış olan,

kendisine özgü güçlü tarafları ve kısıtlılıkları bulunan çok sayıda platform bulunmaktadır. Modelin birinci adımının bu kısmında bu platformlardan en önemlilerinin belirli özelliklerini içeren bir karşılaştırma tablosu karar alternatifi olarak kullanılmak üzere oluşturulmuştur. Bu tablo oluşturulurken Bölüm 2.1.12'de detaylı biçimde verilmiş olan platform özellikleri tabloları kullanılmıştır. Bu tablodan, uygun blokzincir çözümü kararında dikkate alınacak kriterlerin karşılaştırılması aşamasında, Analitik Hiyerarşi Prosesi uygulanırken faydalanılmaktadır.

Çizelge 4.7'de verilmiş olan bu tablo oluşturulurken "teknik", "performans", "güvenlik", "kullanım amacı" ve "nitel" başlıkları altında yer alan toplam 23 özellikten 18'i platformlar birbirleri ile kıyaslanarak derecelendirilmiştir. Kıyaslama yapılırken her bir platform için hazırlanmış olan özellik tablolarındaki veriler kullanımış, bu sayısal verilerin karşılaştırılması sonucunda ilgili veriler "düşük", "orta", "yüksek" gibi derece belirten ifadelere dönüştürülmüş, Çizelge 4.7'de de bu ifadelerin sayısal karşılıklarına yer verilmiştir.

Her bir kritere ve derecelendirme değerlerine ilişkin açıklamalar ayrıca düzenlenerek Çizelge 4.8'de verilmiştir.

Çizelge 4.7. Blokzincir platformu karşılaştırma tablosu

	Özellik	Bitcoin	Ethereum	Hyperledger	Stellar	Quorum	Corda	Multichain	OpenChain	BigchainDB	IOTA	HydraChain	Avalanche	Parity	Kadena
Teknik	Ağa katılım	2	2	1	2	1	1	3	3	3	3	1	3	3	3
	Blokzincir tipi (açık, özel)	1	1	2	1	2	2	3	3	3	3	2	3	3	3
	Hash fonksiyonu	Bölüm 2.1.12'de yer verilmiş olan platform özellik tablolarında yer almakta olup bu tabloya ilave edilmemiştir.													
	Mutabakat mekanizması														
	Yazılım dili														
	Yazılım tipi (açık kaynak kodlu, lisanslı)	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Perfor-mans	İşlem hacmi (saniyede işlem sayısı)[4]	1	1	3	3	2	5	3	5	2	4	2	3	5	4
	Ağ gecikmesi[5]	5	4	2	2	1	1	2	1	1	2	1	2	3	1
	Ölçeklenebilirlik	1	2	3	3	3	3	3	3	3	3	3	3	3	3
	İşlem hızı[6]	1	2	3	3	5	5	3	5	4	3	3	3	3	2
	Blokzincir üçlü çelişkisi (ölçeklenebilirlik, güvenlik, merkezsizlik)	3	3	1	1	1	1	1	1	1	1	1	4	1	4
Güven-lik	DoS ve DDoS saldırılarına direnç	3	3	3	3	1	3	3	3	3	3	3	3	3	3
	Sybil saldırısına direnç	3	3	3	3	3	3	1	3	3	3	3	3	3	3
	Kuantum bilişim riskine direnç	3	3	1[7]	1	1	3	3	3	3	3	3	3	3	3
	Mahremiyet ve gizlilik teknolojisi	3	3	3	3	3	3	3	3	3	3	3	3	3	3
Kullanım amacı	Uygulama türü	2	1	1	2	2	1	1	1	1	1	2	1	1[8]	1
	Akıllı sözleşme desteği	2	1	1	1	1	1	2	1	1	1	1	1	1	1
	Akıllı sözleşme dil desteği	Bölüm 2.1.12'de yer verilmiş olan platform özellik tablolarında yer almaktadır.													
	Token kullanımı	2	1	2	1	1	1	1	1	1	1	1	1	1	1
Nitel	Olgunluk	5	5	5	5	4	4	4	3	4	3	2	3	2	3
	Pazardaki popülarite	5	5	5	4	4	4	4	3	3	4	3	4	4	2
	Geliştirici	Bölüm 2.1.12'de yer verilmiş olan platform özellik tablolarında yer almaktadır.													
	Güvenilirlik	5	5	5	4	4	4	4	2	3	3	2	3	3	2

[4] Bölüm 2.1.12'de yer verilmiş olan özelliklerdeki sayısal değerler birbirleriyle karşılaştırmalı olarak "Çok düşük-1" ile "Çok yüksek-5" aralığında derecelendirilmiştir.
[5] Bölüm 2.1.12'de yer verilmiş olan özelliklerdeki sayısal değerler birbirleriyle karşılaştırmalı olarak "Çok düşük-1" ile "Çok yüksek-5" aralığında derecelendirilmiştir.
[6] Bölüm 2.1.12'de yer verilmiş olan özelliklerdeki sayısal değerler birbirleriyle karşılaştırmalı olarak "Çok düşük-1" ile "Çok yüksek-5" aralığında derecelendirilmiştir.
[7] Kuantum sonrası kriptografi için dijital imza altyapısı qTESLA'nın yakın dönemde hibrit bir çözüm olarak kullanılabileceği tahmin edilmektedir.
[8] Daha çok birden fazla blokzincir yapısının bir arada kullanımı için uygundur

Çizelge 4.7'de yer alan özellikler ve her bir özelliğin alternatiflere göre değerlerine ilişkin açıklamalar Çizelge 4.8'de verilmiştir:

Çizelge 4.8. Blokzincir platformu karşılaştırma tablosu açıklamaları

	Özellik	***Seçim kriteri mi?***	***Açıklama***
Teknik	Ağa katılım	Hayır (ya da başl. 0-1 seçimi)	İzin gerektiren (1), İzin gerektirmeyen (2), Her iki tipte de konfigüre edilebilir (3)
	Blokzincir tipi (açık, özel)	Hayır (ya da başl. 0-1 seçimi)	Açık (1), Özel (2), Her iki tipte de konfigüre edilebilir (3)
	Hash fonksiyonu	Hayır	Güvenlik özelliği ile ilintilidir. Güvenlik başlığı altında kriter olarak değerlendirilmektedir.
	Mutabakat mekanizması	Hayır	Performans ve güvenlik özellikleri ile ilintilidir.
	Yazılım dili	Hayır	Kullanılan yazılım dillerine ilişkin detaylar Bölüm 2.1.12'de verilmiştir.
	Yazılım tipi (açık kaynak kodlu, lisanslı)	Opsiyonel	Açık kaynak kodlu (1), lisanslı (2), kendi bünyesinde geliştirme (3), diğer (4)
Performans	İşlem hacmi (saniyede işlem sayısı)	Evet	Çok düşük (1), Düşük (2), Orta (3), Yüksek (4) Çok yüksek (5)
	Ağ gecikmesi	Evet	Çok düşük (1), Düşük (2), Orta (3), Yüksek (4) Çok yüksek (5)
	Ölçeklenebilirlik	Evet	Düşük (1), Orta (2), Yüksek (3)
	İşlem hızı	Evet	Çok düşük (1), Düşük (2), Orta (3), Yüksek (4) Çok yüksek (5)
	Blokzincir üçlü çelişkisi (ölçeklenebilirlik, güvenlik, merkezsizlik)	Evet	Ölçeklenebilir ve güvenli ama merkezi (1), Ölçeklenebilir ve merkezsiz ama güvensiz (2), Güvenli ve merkezsiz ama ölçeklenebilir değil (3), Ölçeklenebilir, güvenli ve merkezsiz (4)
Güvenlik	DoS ve DDoS saldırılarına direnç	Opsiyonel	Düşük (1), Orta (2), Yüksek (3)
	Sybil saldırısına direnç	Opsiyonel	Düşük (1), Orta (2), Yüksek (3) Blokzincir sisteminin açık, özel olması, kullanılan mutabakat mekanizması gibi özellikler dikkate alınarak
	Kuantum bilişim riskine direnç	Opsiyonel	Düşük (1), Orta (2), Yüksek (3) Kullanılan anahtarların tekrar kullanılması, tek kullanımlık anahtar kullanımı, blok oluşturma zamanı, kullanılan hash ve şifreleme algoritmaları gibi faktörler dikkate alınarak değerlendirilmektedir.
	Mahremiyet ve gizlilik teknolojisi	Opsiyonel	Düşük (1), Orta (2), Yüksek (3) Platformda kullanılan kriptografik fonksiyonlar, anonimlik tasarımı, işlemlerin açık-gizli anahtarlarla ilişkilendirilmesi gibi özellikler dikkate alınarak
Kullanım amacı	Uygulama türü	Evet - başlangıç 0 1 seçimi	Genel amaçlı (1), Sadece belirli işlemler için (2) – Seçim "2" ise "kullanım senaryosuna uygun mu?" sorusu sorulacaktır.
	Akıllı sözleşme desteği	Evet - başlangıç 0 1 seçimi	Evet (1), Hayır (2)
	Akıllı sözleşme dil desteği	Hayır	Kullanılan yazılım dillerine ilişkin detaylar Bölüm 2.1.12'de verilmiştir.
	Token kullanımı	Evet - başlangıç 0 1 seçimi	Evet (1), Hayır (2)
Nitel	Olgunluk	Evet	Çok düşük (1), Düşük (2), Orta (3), Yüksek (4) Çok yüksek (5)
	Pazardaki popülarite	Evet	Çok düşük (1), Düşük (2), Orta (3), Yüksek (4) Çok yüksek (5)
	Geliştirici	Hayır	Olgunluk, popülarite ve güvenilirlik kriterlerinin değerlendirilmesinde kullanılmaktadır.
	Güvenilirlik	Evet	Çok düşük (1), Düşük (2), Orta (3), Yüksek (4) Çok yüksek (5)

Karar ağaçları

Modelin ilk adımının bu faaliyetinde literatürde yer alan blokzincir çözümünün kullanım kararına ilişkin karar ağaçları araştırılarak yeni bir karar ağacı oluşturulmaktadır. İncelenen karar ağaçları ile model kapsamında kullanılmak üzere geliştirilmiş olan karar ağacı Şekil 4.2'de verilmiştir.

Çok Kriterli Karar Verme (ÇKKV) metotları

Modelde platform alternatiflerinin kullanıcı tarafından seçilen kriterlere göre birbirleri ile karşılaştırılarak önceliklerine göre sıralanması için en uygun metodun seçilmesi için ÇKKV metotları araştırılmış, modelde kullanımına karar verilmiş olan Analitik Hiyerarşi Prosesi metodu da dâhil olmak üzere tüm metotlar işlem adımları ile birlikte Bölüm 2.7'de verilmiştir.

4.1.2. Adım 2. Kural Tabanı

Bu adımda, ilk adımda derlenen bilgiler analiz edilerek blokzincir çözümünün kullanılabilirliği ve kullanılabilir çözümün temel özellikleri konularında karar noktaları için kurallar oluşturulmaktadır. İlk adımda elde edilen nesnel bilgiler ışığında oluşturulan bu kurallar karar verilecek sürece ilişkin toplanacak veriler ile birlikte değerlendirilmek üzere oluşturulmaktadır.

İlk adımda derlenmiş olan bilgilerde değişiklik meydana gelmesi halinde bu adımdaki kurallarda da değişiklik gereksinimi olmakla birlikte, bunların modelin işleyişine etkisi bulunmamaktadır.

Kural tabanı adımının girdileri, bu adımda gerçekleştirilen işlemler ve bu işlemler sonucunda elde edilen çıktılar alt başlıklar halinde aşağıda sıralanmaktadır.

<u>Girdiler</u>

İkinci adımın girdilerini ilk adımdaki çıktıların tamamı oluşturmaktadır. Adım 1'de detayları verilmiş olan bu girdiler aşağıdaki biçimdedir:

- Temel özellikler listesi
- Avantajlar ve güçlü yönler listesi
- Dezavantajlar ve kısıtlılıklar listesi
- Potansiyel kullanım alanları ve mevcut uygulamalar listesi
- Platform karşılaştırma tablosu
- Karar ağacı
- Çok Kriterli Karar Verme (ÇKKV) metotları - AHP

İşlemler

Modelin bu adımı, ilk adımda elde edilmiş olan bilgilerin sınıflandırılması ve analizine dayanmaktadır. Bu adımdaki kurallar temel olarak iki gruptadır; blokzincir çözümünün kullanılabilir olup olmadığına yönelik karar kuralları ve kullanılabilir olması halinde uygun mimarının seçilmesine yönelik karar kuralları.

Blokzincir çözümünün kullanılabilir olup olmadığına yönelik karar kuralları:

- Bu kurallar ilk adımda çıktı olarak elde edilmiş olan temel özellikler, güçlü yönler ve avantajlar, dezavantaj ve kısıtlılıklar, potansiyel kullanım alanları ve mevcut uygulamalar listelerinde yer alan veriler bir araya getirilip değerlendirilerek oluşturulmuş olup nihai karar kuralları bir karar ağacı olarak tasarlanmıştır. Bu karar ağacında çoğunlukla "evet" ve "hayır" cevabı verilebilen sorular yer almaktadır.

Uygun mimarinin seçilmesine yönelik karar kuralları:

- Bu kurallar da kendi içerisinde ikiye ayrılmaktadır;
  - Kullanıcının kesinlikle belirli bir özellik belirterek cevaplandırdığı nitelikler: Bu nitelikler Çizelge 4.9'da verilmiş olup herhangi bir seçim yapılmaması halinde tüm alternatifler değerlendirmeye alınmaktadır.

Çizelge 4.9. Blokzincir platformunun niteliklerine ilişkin seçenekler (kesin özellik)

Nitelik	Seçim zorunlu mu?	Seçenekler	Karar
Ağa katılım	Opsiyonel	İzin gerektiren (1), İzin gerektirmeyen (2), Her iki tipte de konfigüre edilebilir (3)	
Blokzincir tipi (açık, özel)	Opsiyonel	Açık (1), Özel (2), Her iki tipte de konfigüre edilebilir (3)	
Yazılım tipi (açık kaynak kodlu, lisanslı)	Opsiyonel	Açık kaynak kodlu (1), lisanslı (2), kendi bünyesinde geliştirme (3), diğer (4)	

Nitelik	Seçim zorunlu mu?	Seçenekler	Karar
Uygulama türü	Zorunlu	Genel amaçlı (1), Sadece belirli işlemler için (2)*	
Akıllı sözleşme desteği	Opsiyonel	Evet (1), Hayır (2)	
Token kullanımı	Opsiyonel	Evet (1), Hayır (2)	
* Kullanım senaryosu belirtilecektir			

- Kullanıcının önem derecesi ya da öncelik belirttiği nitelikler: Çizelge 4.10'da verilmiş olan bu nitelikler ise seçim kriteri olarak değerlendirilecek olup birbirlerine göre önem derecelerine göre çözüm alternatifleri değerlendirilecektir. Herhangi bir seçim yapılmaması halinde tüm alternatifler değerlendirmeye alınmaktadır.

Çizelge 4.10. Blokzincir platformunun niteliklerine ilişkin seçenekler (derece belirten)

Nitelik	Seçim zorunlu mu?	Seçenekler	Karar
İşlem hacmi (saniyede işlem sayısı)	Opsiyonel	Çok düşük (1), Düşük (2), Orta (3), Yüksek (4) Çok yüksek (5)	
Ağ gecikmesi	Opsiyonel	Çok düşük (1), Düşük (2), Orta (3), Yüksek (4) Çok yüksek (5)	
Ölçeklenebilirlik	Opsiyonel	Çok düşük (1), Düşük (2), Orta (3), Yüksek (4) Çok yüksek (5)	
İşlem hızı	Opsiyonel	Çok düşük (1), Düşük (2), Orta (3), Yüksek (4) Çok yüksek (5)	
Blokzincir üçlü çelişkisi (ölçeklenebilirlik, güvenlik, merkezsizlik)	Hangisinden feragat edilebileceği seçilecektir	( ) Merkezsizlik ( ) Ölçeklenebilirlik ( ) Güvenlik ( ) Hiçbiri	
DoS ve DDoS saldırılarına direnç	Opsiyonel	Düşük (1), Orta (2), Yüksek (3)	
Sybil saldırısına direnç	Opsiyonel	Düşük (1), Orta (2), Yüksek (3)	
Kuantum bilişim riskine direnç	Opsiyonel	Düşük (1), Orta (2), Yüksek (3)	
Mahremiyet ve gizlilik teknolojisi	Opsiyonel	Düşük (1), Orta (2), Yüksek (3)	
Olgunluk	Opsiyonel	Çok düşük (1), Düşük (2), Orta (3), Yüksek (4) Çok yüksek (5)	
Pazardaki popülarite	Opsiyonel	Çok düşük (1), Düşük (2), Orta (3), Yüksek (4) Çok yüksek (5)	
Güvenilirlik	Opsiyonel	Çok düşük (1), Düşük (2), Orta (3), Yüksek (4) Çok yüksek (5)	

İkinci adımda yürütülen bir diğer faaliyet MoSCoW metodu ile önceliklerin belirlenmesidir. MoSCoW metodu öncelikleri belirlemek ve analiz etmek için kullanılan bir yöntemdir. Blokzincir çözümü için gereksinimlerin ortaya konulmasında kullanılmaktadır. Bu metot İngilizce "Must have", "Should have", "Could have" ve "Won't have" ifadelerinin baş harflerinden oluşmuş olup her bir ifadenin açılımı aşağıdaki biçimdedir:

- Olması gerekenler (Must have): Aranan çözümün mutlaka taşıması gereken özellikleri ifade eder. Genellikle en kolay tanımlanan özelliklerdir. Bu özelliği taşımayan alternatifler olası çözümler listesinden kaldırılmaktadır.
- Olması faydalı olanlar (Should have): Olması çözüm için mutlaka gerekmemekle birlikte çözüme büyük katkı sağlayan, olması gerekenlerden biraz daha az öneme sahip özelliklerdir. Temel özellik olmamakla birlikte, istek ve beklentileri karşılamaya yarayacak özelliklerdir.
- Olması iyi karşılananlar (Could have): Olması halinde çözüme değer katan özelliklerdir. Temel özellikler ile çözüme değer katan özelliklere ek olarak ekstra konfor sağlayan özellikler bu gruba girmektedir.
- Olmaması gerekenler (Won't have): Çözümün taşımaması gereken özelliklerdir.

Çıktılar

Modelin sonraki aşamalarında kullanılmak üzere bu adımda elde edilmiş olan çıktılar aşağıdaki biçimdedir:

Blokzincir kullan-kullanma listesi

Detaylı karar adımlarına geçmeden önce, blokzincir çözümünün uygulanabilirliğine ilişkin kesin özellikler ve kullanım örnekleri dikkate alınarak seçilen süreç için bir değerlendirme yapılarak sonraki adımlara geçilip geçilmeyeceğine karar vermek üzere bir ön eleme adımıdır. Buna göre, blokzincir çözümünün kullanılabilir olduğu, sonraki adımlar yürütülerek karar verilebileceği ya da blokzincirin seçilen süreç için kullanılamaz olduğu kararı için kullanılacak liste Çizelge 4.11'de verilmiştir.

Çizelge 4.11. Blokzincir kullan-kullanma listesi

Soru	Seçenekler	Değerlendirme
Kullanım senaryosu şunlardan birini içeriyor mu?*	Dijital kimlik yönetimi Dijital sertifika (diploma, transkript, eğitim belgesi vb.) Elektronik oylama Gayrimenkul kayıt sistemi Ürün takibi (gıda, ilaç vb.) İhale ve satınalma sistemi İzlenebilirlik ve orijinallik kontrolü Kişisel kayıtların yönetimi (sağlık, finans vb.) Mesajlaşma sistemi Noter onayı	Hayır ise blokzincir kullanımı önerilmemekle birlikte sürecin özelliklerine göre modelin diğer adımları izlenerek karar verilmelidir.

Soru	Seçenekler	Değerlendirme
	Sosyal yardımların dağıtılması Tedarik zinciri yönetimi Telif hakları yönetimi	
Kullanım senaryosu şunlardan en az birini gerektiriyor mu?	Çok yüksek veri hacmi, Çok yüksek işlem hızı, Çok yüksek işlem sayısı, Yüksek performans, Veri silme, değiştirme ya da güncelleme	Evet ise açık blokzincir kullanımı önerilmez
* Blokzincirin mevcut uygulamaları içerisinden kamu hizmetlerine uygun olanlar seçilmiştir		

Blokzincir kullanım kararı için karar ağacı

Bölüm 4.1'de yer verilmiş olan karar ağacı (Bkz. Şekil 4.2) blokzincir çözümünün kullanılabilir olup olmadığı kararı için kullanılmaktadır. Buna göre, karar ağacında yer alan 12 soruya verilen yanıtlar sonucunda "blokzincir kullanımı önerilmez", "kullanılması önerilmemekte olup blokzincir kullanımının sağlayacağı fayda iyi analiz edilmelidir" ve "blokzincir kullanılabilir" kararlarından biri çıktı olarak elde edilmektedir.

MoSCoW özellik listesi

Blokzincir çözümünün kullanımına ve kullanılması halinde sahip olacağı özelliklere karar vermek için değerlendirilecek nitelikler Çizelge 4.12'de verilmiştir. Bu listede yer verilmiş olan her bir nitelik, seçilen süreç dikkate alınarak değerlendirilmekte, bu değerlendirme sonucuna göre M (olması gereken) ve W (olmaması gereken) özellikler alternatiflerin doğrudan elenmesinde kullanılmaktadır. S (olması faydalı olanlar) ve C (olması iyi karşılananlar) ise eleme sonrası kalan alternatiflerin önceliklendirilmesinde kriter olarak değerlendirilmektedir. Burada, S olarak seçilen nitelikler C olarak seçilenlere göre daha önceliklidir.

Çizelge 4.12. Blokzincir çözümünün değerlendirilmesinde kullanılan nitelikler

Nitelik Grubu	Nitelik	Seçenek
Ağa katılım	İzin gerektiren	MoSCoW
	İzin gerektirmeyen	MoSCoW
	Her iki tipte de konfigüre edilebilir	MoSCoW
Blokzincir tipi (açık, özel)	Açık blokzincir	MoSCoW
	Özel blokzincir	MoSCoW
	Her iki tipte de konfigüre edilebilir	MoSCoW
Yazılım tipi	Açık kaynak kodlu	MoSCoW
	Lisanslı	MoSCoW
	Kendi bünyesinde geliştirme	MoSCoW
Güvenlik	DoS ve DDoS saldırılarına direnç	MoSCoW

Nitelik Grubu	Nitelik	Seçenek
	Sybil saldırısına direnç	MoSCoW
	Kuantum bilişime direnç	MoSCoW
	Mahremiyet ve gizlilik teknolojisi	Düşük, Orta, Yüksek
Kullanım amacı	Uygulama türü	Genel, Özel
	Akıllı sözleşme desteği	MoSCoW
	Token kullanımı	MoSCoW
Performans	İşlem hacmi	Çok düşük – Çok yüksek
	Ağ gecikmesi	Çok düşük – Çok yüksek
	İşlem hızı	Çok düşük – Çok yüksek
Diğer	Olgunluk	Çok düşük – Çok yüksek
	Popülarite	Çok düşük – Çok yüksek
	Güvenilirlik	Çok düşük – Çok yüksek
Blokzincir üçlü çelişkisi	Ölçeklenebilirlik	MoSCoW
	Güvenlik	MoSCoW
	Merkezsizlik	MoSCoW

Çizelge 4.12'de verilmiş olan nitelikler için MoSCoW seçeneklerinden birini tercih etmek zorunlu değildir. Herhangi bir seçim yapılmayan özellikler, bulunması ya da bulunmamasının bir fark yaratmayacağı biçiminde değerlendirilmektedir.

İkili karşılaştırmalar için kriter listeleri

MoSCoW özellik listesi dışında kalan, seçenek olarak dilsel değişken (çok düşük, çok yüksek, gibi) içeren özellikler ise doğrudan ikili karşılaştırmalarda kullanılmak üzere belirlenmiş olup bu özellikler Çizelge 4.13'te verilmiştir.

Çizelge 4.13. Blokzincir platformları için ikili karşılaştırma nitelikleri

Nitelik Grubu	Nitelik	Seçenek
Güvenlik (opsiyonel)	Mahremiyet ve gizlilik teknolojisi	Düşük, Orta, Yüksek
Performans	İşlem hacmi	Çok düşük – Çok yüksek
	Ağ gecikmesi	Çok düşük – Çok yüksek
	İşlem hızı	Çok düşük – Çok yüksek
Diğer	Olgunluk	Çok düşük – Çok yüksek
	Popülarite	Çok düşük – Çok yüksek
	Güvenilirlik	Çok düşük – Çok yüksek

Burada, dikkat edilmesi gereken konu ikili karşılaştırma listesinin dinamik ve değişken olduğudur. Bir önceki adımda belirlenmiş olan MoSCoW listesi çıktılarına göre, bu listeye "S" ve "C" olarak seçilen özellikler de eklenmelidir. Örneğin, MoSCoW listesinde yer alan "Güvenlik" ana başlığı altındaki "DDoS saldırısına direnç" için "S" seçilmişse bu nitelik ikili karşılaştırma listesine eklenecektir.

Analitik Hiyerarşi Prosesi (AHP) işlem adımları

AHP metodunda işlemler kriterler ve alternatifler üzerinden gerçekleştirilmektedir. Bu nedenle, AHP işlem adımlarına geçmeden önce, kriterler ve alternatifler önceki adımlardaki elemeler ve MoSCoW özellik listeleri kullanılarak nihai hale getirilmektedir. Örneğin, blokzincir tipinin "özel" olması isteniyorsa, açık blokzincir platformları (Bitcoin gibi) alternatifler içerisinden çıkarılmaktadır. Daha sonra, kriterler belirlenirken, Çizelge 4.13'te verilmiş olan sabit seçim kriterlerine MoSCoW özellik listesinden ilave yapılarak nihai kriter listesi oluşturulmaktadır. Bu ön çalışmaların ardından AHP metodu uygulanmaktadır. Buna göre, Bölüm 2.7.3'te detaylı biçimde verilmiş olan işlem adımları izlenmekte olup bu işlem adımları kısaca aşağıdaki biçimdedir:

Adım 1. Üzerinde karar verilecek durumun ve amacın tanımlanması: Bu adımda karar problemi tanımlanmakta, karara etki eden unsurlar ve alternatifler belirlenmektedir. Karar işlemlerini doğrudan etkilediği için çok büyük önem taşıyan bu tanımlamalar AHP işlemlerine altlık sağlayacak biçimde, problem, amaç, kriterler, kriterlerin problemin çözümüne ve hedefe ulaşılmasına verecek katkıları bakımından önem dereceleri ve alternatifleri içermektedir.

Adım 1.1. Problem ve hedefin tanımlanması: Bu aşamada, çözüm aranan problem tarif edilerek hedefler kriter ve özellik listelerinde yer verilen nitelikler kullanılarak tanımlanmaktadır. Örneğin;
"Seçilen süreç için veri sızıntılarına karşı dirençli, yüksek işlem hızı sağlayan, işlem hacminin sürekli ve yoğun olmadığı, daha önce denenmiş ve başarısı kanıtlanmış bir blokzincir çözümü aranmaktadır."

Adım 1.2. Blokzincir çözüm alternatiflerinin belirlenmesi: Bu adımda, Çizelge 4.12'de verilmiş olan özelliklerden mutlaka olması gerekenler (Must have) ve kesinlikle olmaması gerekenler (Won't have) seçilerek bunlara göre Çizelge 4.7'de verilmiş olan platform karşılaştırma tablosunda yer alan 14 platform alternatifi değerlendirilmekte, uygun olmayanlar elenerek nihai alternatif listesi oluşturulmaktadır. Buna göre, MoSCoW listesinden kesinlikle olması veya olmaması istenen özelliklerin seçilme durumuna göre, her bir nitelik için uygun platformlar ayrı ayrı seçilmekte olup nihai platform listesi bu seçimlere

ilişkin kümelerin kesişim kümesidir. Bu kesişim kümesini belirlemek için Çizelge 4.14 kullanılmakta olup bu çizelgenin kullanımına ilişkin kurallar aşağıda ayrıca verilmiştir.

Çizelge 4.14. MoSCoW listesine göre platform değerlendirme tablosu

		Seçim (0, 1)	M/W	Bitcoin	Ethereum	Hyperledger	Stellar	Quorum	Corda	Multichain	OpenChain	BigchainDB	IOTA	HydraChain	Avalanche	Parity	Kadena
Ağa katılım	İzin gerektiren																
	İzin gerektirmeyen																
	Her iki tipte de konfigüre edilebilir																
Blokzincir tipi	Açık blokzincir																
	Özel blokzincir																
	Her iki tipte de konfigüre edilebilir																
Yazılım tipi	Açık kaynak kodlu																
	Lisanslı																
	Kendi bünyesinde geliştirme																
Güvenlik	DoS ve DDoS saldırılarına direnç																
	Sybil saldırısına direnç																
	Kuantum bilişime direnç																
Kullanım amacı	Akıllı sözleşme desteği																
	Token kullanımı																
Üçlü çelişki	Ölçeklenebilirlik																
	Güvenlik																
	Merkezsizlik																

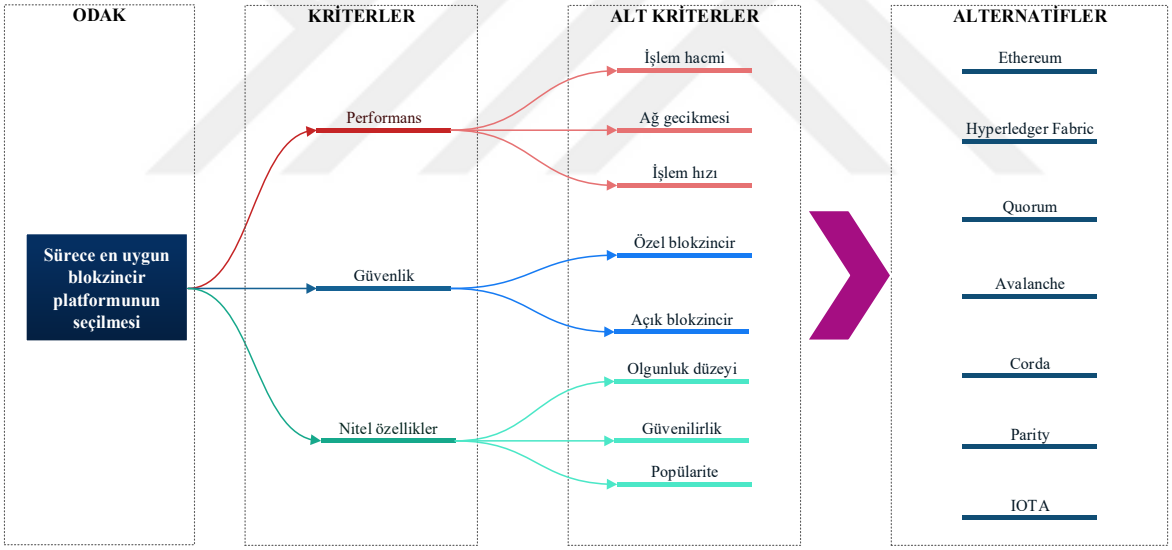
Çizelge 4.14'ün doldurulmasına ilişkin kurallar:

1. İkinci sütunda, seçilen, yani MoSCoW listesinde tercih belirtilen özellikler için "1", seçilmeyen, yani MoSCoW listesinde tercih belirtilmeyen özellikler için ise "0" kullanılacaktır.
2. İlk sütun değeri "1" olan satırlar alternatiflerin değerlendirilmesinde kullanılacak, ilk sütun değeri "0" olan satırlar ise dikkate alınmayacaktır.
3. İlk sütun değeri "1" olan satırlar için, ikinci sütunda mutlaka olması istenen özellik ise "M", mutlaka olmaması istenen özellik ise "W" kullanılacaktır.
4. Platform karşılaştırma tablosu kullanılarak, ilk sütun değeri "1" olan her bir satır için, her bir alternatif, ikinci sütundaki "M" ya da "W" seçimine göre değerlendirilecek, özellik karşılanıyorsa "1", karşılanmıyorsa "0" değeri ilgili hücreye yazılacaktır.
5. İstenen özelliği karşılamayan, ya da hücre değeri "0" olan alternatifler elenecektir.

6. Tüm elemeler gerçekleştirildikten sonra kalan alternatifler AHP işlem adımlarında kullanılmak üzere nihai alternatifler olarak listelenecektir.

Adım 2. Hiyerarşik yapının oluşturulması (çözüm alternatiflerinin değerlendirilmesinde kullanılacak kriterlerin belirlenmesi): Bu adımda, Çizelge 4.13'te verilmiş olan kriterlere Çizelge 4.12'deki MoSCoW özellik listesinden "S" ve "C" olarak seçilenler eklenerek nihai kriter listesi oluşturulmaktadır. Daha sonraki adımlarda kullanılmak üzere, kriter listesine MoSCoW listesinden ilave edilen niteliklerden "S" olarak seçilenlerin, "C" olarak seçilenlere göre daha önemli olduğu hatırlanmalıdır.

Burada, karar verilecek durum ve amaç, alternatifler ve kriterler belirlendikten sonra, bu üçü arasındaki ilişkiyi göstermek üzere hiyerarşik yapı oluşturularak şematize edilmektedir. Şekil 4.13'te örnek bir hiyerarşik yapı verilmiştir.



Şekil 4.3. AHP için örnek hiyerarşik yapı

Adım 3. İkili karşılaştırma matrislerinin oluşturulması: Hem her kriterin birbiri ile ikili karşılaştırması hem de tüm alternatiflerin her bir kritere göre birbirleri ile karşılaştırılması için matris işlemlerinin gerçekleştirildiği adımdır.

Adım 4. Matrislerin normalize edilmesi: Detayları Bölüm 2.7.3'te verilmiştir.

Adım 5. Öncelik vektörünün hesaplanması: Detayları Bölüm 2.7.3'te verilmiştir.

Adım 6. Tutarlılık analizinin yapılması: Detayları Bölüm 2.7.3'te verilmiştir.

Adım 7: Karar alternatifleri öncelik vektörünün hesaplanması: Detayları Bölüm 2.7.3'te verilmiştir.

Adım 8: Karar alternatiflerinin ağırlıklarına göre sıralanması: Detayları Bölüm 2.7.3'te verilmiştir.

4.1.3. Adım 3. Süreç seçimi, bilgi toplama ve veri girişi

Bu adım modele dışarıdan bilgi girişinin sağlandığı, hesaplamalarda kullanılacak verilerin süreç sahibinden temin edilerek derlendiği adımdır. Bilginin sistematik bir biçimde toplanması için standart bir soru formu oluşturulmuştur. Oluşturulan soru formu ile hem sürecin mevcut durumu hakkında bilgi edinilmekte, hem de yeni tasarlanacak sistemden beklentiler alınmaktadır.

Süreç seçimi, bilgi toplama ve veri girişi adımının girdileri, bu adımda gerçekleştirilen işlemler ve bu işlemler sonucunda elde edilen çıktılar alt başlıklar halinde aşağıda sıralanmaktadır.

<u>Girdiler</u>

Kullanıcı ya da süreç sahibinden alınacak bilgiler için oluşturulan form şablonları, önceki adımlarda hazırlanmış olan listeler ve sürecin mevcut durumuna ilişkin şematik gösterimler bu adımın girdilerini oluşturmakta olup aşağıdakileri içermektedir:

a) Süreç Bilgi Toplama Formu
b) Süreç akış şeması
c) MoSCoW özellik listesi
d) İkili karşılaştırmalar için kriter listeleri

Süreç ve ilgili kurum hakkında bilgi toplamak için hazırlanmış olan girdi formu (Süreç Bilgi Toplama Formu) Ek-1'de verilmiştir. Süreç akış şeması eğer mevcut ise doğrudan girdi olarak alınmakta, değilse edinilen bilgiye göre hazırlanmaktadır. Diğer girdiler ise

(MoSCoW özellik listesi, İkili karşılaştırmalar için kriter listeleri) modelin ikinci adımının çıktıları arasında yer alan listelere, bu adımda sürece ilişkin olarak elde edilen bilgilerin ilave edilmesi ile oluşturulmaktadır.

İşlemler

Modelin bu adımında önceden hazırlanmış olan soru formları ile yapılandırılmış bir biçimde bilgi toplanmakta, toplanan bilgiler kullanılarak mevcut ve beklenen durum çıkarılarak gap analizi yapılmaktadır. Yine bu bilgilerden faydalanılarak sürece ilişkin tercih ve öncelikler çıkarılmakta, ikinci adımda hazırlanmış olan MoSCoW listesine nihai hali verilmekte, çözüm alternatiflerinin öncelik hesaplanması için kullanılacak kriter derecelendirmesi gerçekleştirilmektedir.

Bu aşamada, Süreç Bilgi Formunda (Ek-1) yer verilen soruların yanıtlarının kullanılacağı alanlar Çizelge 4.15'te verilmiştir:

Çizelge 4.15. Süreç Bilgi Formu çıktılarının kullanım alanları

Soru no	Konu	Kullanılacağı alan
1	Süreçte rol alan kurum/birimler ve rolleri	Süreç tasarımı
2	Süreç işlem hacmi	Platform karşılaştırma tablosu/kriter ikili karşılaştırma listesi
3	Süreç tarafından üretilen/depolanan veri miktarı	Süreç tasarımı
4	Süreç işlem hızı	Platform karşılaştırma tablosu/kriter ikili karşılaştırma listesi
5	Blokzincir üçlü açmazı	Platform karşılaştırma tablosu/kriter ikili karşılaştırma listesi
6	Süreç veri içeriği	Süreç tasarımı - mimari
7	Veri sınıflandırma	Süreç tasarımı – mimari
8	Sürecin işleyişi	Süreç tasarımı
9	Hassas, gizli ya da kritik bilgi ya da veri kullanımı	Süreç tasarımı – mimari
10	Dış bilgi gereksinimi	Süreç tasarımı – mimari
11	Mevcut mevzuat	Süreç tasarımı – mimari
12	Fonksyionel gereksinimler	Blokzincir çözümü kullanım kararı
13	Fonksiyonel olmayan gereksinimler	Platform karşılaştırma tablosu/kriter ikili karşılaştırma listesi
14	Mevcut süreç/faaliyetle ilgili problemler ya da iyileştirilebilir noktalar	Süreç tasarımı – mimari

Süreç hakkında edinilen sayısal bilgilerin dilsel değişkenlere çevirilmesinde blokzincir platformlarının özelliklerinden çıkarılmış olan minimum ve maksimum değerler temel alınmaktadır. Buna göre, işlem hacmi, ağ gecikmesi ve işlem hızı parametreleri için minimum ve maksimum değerler Çizelge 4.16'da verilmiştir.

Çizelge 4.16. Süreç performans parametreleri için maksimum ve minimum değerler

Sürecin performans parametreleri	**Min**	**Max**
İşlem hacmi (saniyede işlem sayısı)	4	20 000
Ağ gecikmesi	Yok	1 saat
İşlem hızı	Anlık	10 dakika

Çözüm alternatifi için seçilen 14 platformun özellikleri dikkate alınarak her bir performans parametresi için aralıklar belirlenmiş olup seçilen sürecin işlem hacmi, ağ gecikmesi ve işlem hızı özelliklerinin çok düşük ile çok yüksek arasında derecelendirmesinde kullanılmak üzere Çizelge 4.17 oluşturulmuştur.

Çizelge 4.17. Süreç performans parametreleri için eşik değerler

Sürecin performans parametreleri	**Çok düşük (1)**	**Düşük (2)**	**Orta (3)**	**Yüksek (4)**	**Çok yüksek (5)**
İşlem hacmi (saniyede işlem sayısı)	< 100	≥ 100 & < 1 000	≥100 & < 5 000	≥5 000 & < 12 500	≥ 12 500
Ağ gecikmesi	< 1 sn	≥ 1 sn & < 5 sn	≥ 5 sn & < 5 dak	≥ 5 dak & < 30 dak	≥ 30 dak
İşlem hızı	≥ 1 dak	≥ 15 sn &< 1 dak	≥ 3 sn & < 15 sn	≥ 1 sn & < 3 sn	< 1sn

Bu adımda, daha sonra, önce Çizelge 4.9'da verilmiş olan blokzincir platformunun niteliklerine ilişkin seçenekler (kesin özellik) tablosu, ardından Çizelge 4.10'da verilmiş olan blokzincir platformunun niteliklerine ilişkin seçenekler (derece belirten) tablosu kullanıcı tercihleri ve beklenen özellikler doğrultusunda doldurulmaktadır. Kesin özellikler ile derece belirten özelliklere ilişkin veri girişinden sonra son olarak Çizelge 4.12'de verilmiş olan blokzincir çözümünün değerlendirilmesinde kullanılan nitelikler tablosunda MoSCoW özelliklerine ilişkin seçimler yapılmaktadır. Kullanıcının bu seçimleri gerçekleştirmesi için Çizelge 4.12'den türetilmiş olan Çizelge 4.18 aşağıda verilmiştir.

Çizelge 4.18. MoSCoW metodu – önceliklerin belirlenmesi için kullanılan seçim listesi

Nitelik Grubu	**Nitelik**	**Seçenek (MoSCoW)**			
		M	**S**	**C**	**W**
Ağa katılım	İzin gerektiren				
	İzin gerektirmeyen				
	Her iki tipte de konfigüre edilebilir				
Blokzincir tipi (açık, özel)	Açık blokzincir				
	Özel blokzincir				
	Her iki tipte de konfigüre edilebilir				
Yazılım tipi	Açık kaynak kodlu				
	Lisanslı				

Nitelik Grubu	Nitelik	Seçenek (MoSCoW)			
		M	S	C	W
	Kendi bünyesinde geliştirme				
Güvenlik	DoS ve DDoS saldırılarına direnç				
	Sybil saldırısına direnç				
	Kuantum bilişime direnç				
	Akıllı sözleşme desteği				
	Token kullanımı				
Blokzincir üçlü çelişkisi	Ölçeklenebilirlik				
	Güvenlik				
	Merkezsizlik				

***M**: Olması gerekenler; **S**: Olması faydalı olanlar; **C**: Olması iyi karşılananlar; **W**: Olmaması gerekenler*

MoSCoW seçimlerinin ardından, S (olması faydalı olanlar) ve C (olması iyi karşılananlar) olarak seçilen nitelikler Çizelge 4.13'te verilmiş olan blokzincir platformları için ikili karşılaştırma nitelikleri tablosuna eklenerek nihai ikili karşılaştırma nitelik tablosu oluşturulmaktadır.

Bu adımda son olarak, hesaplama adımında yürütülen Analitik Hiyerarşi Prosesinde kullanılan kriterlerin birbirlerine göre önem derecelerinin belirlenmesi işlemi gerçekleştirilmektedir. Bu işlem, Çizelge 4.13 ile MoSCoW özellik listesi kullanılarak oluşturulmuş olan nihai kriterlerin Çizelge 2.41'de verilmiş olan AHP için temel ölçek tablosunda yer alan "mutlak ölçekte önem kuvveti" değerleri kullanılarak birbirlerine göre önem derecelerinin belirlenmesini içermektedir. Bu işlem aynı zamanda AHP'nin üçüncü adımına denk gelen ikili karşılaştırma matrislerinin oluşturulmasıdır ve Çizelge 4.19'da bir örneği verilmiştir.

Çizelge 4.19. Örnek ikili karşılaştırma matrisi (Model adımı 3)*

Kriterler	Kriter-1	Kriter-2	Kriter-3	Kriter-4	Kriter-5
Kriter-1	1	2	5	7	7
Kriter-2	1/2	1	3	4	6
Kriter-3	1/5	1/3	1	1	3
Kriter-4	1/7	1/4	1	1	5
Kriter-5	1/7	1/6	1/3	1/5	1

**Hücrelerdeki değerler satırda yer alan kriterlerin sütunda yer alan kriterlere göre önem derecesini ifade etmektedir.*

Çıktılar

Modelin sonraki aşamalarında kullanılmak üzere bu adımda elde edilmiş olan çıktılar aşağıdaki biçimdedir:

Süreç bilgileri (gap analizi sonuçları)

Mevcut süreç bilgileri ile beklenen özellikler ve gap analizi sonucunda önerilen yeni süreç işlem adımları detayları ile birlikte, blokzincir mimarisine uygun biçimde hazırlanmaktadır.

MoSCoW yanıt listesi (Çizelge 4.18)

Önceki adımda hazırlanmış olan aşağıdaki tablolar gerekli veri girişi yapılarak bir sonraki adımdaki hesaplama işlemlerine hazır hale getirilmektedir:

- Blokzincir platformunun niteliklerine ilişkin seçenekler (kesin özellik) tablosu
- Blokzincir platformunun niteliklerine ilişkin seçenekler (derece belirten) tablosu
- Blokzincir çözümünün değerlendirilmesinde kullanılan nitelikler tablosu (MoSCoW)
- Blokzincir platformları için ikili karşılaştırma nitelikleri tablosu

Kriter önem sırası/derecesi

Blokzincir platformu seçimine esas olan kriterlerin birbirlerine göre önem dereceleri Çizelge 2.41'de verilmiş olan AHP için temel ölçek tablosu temel alınarak liste ve matris biçiminde hazırlanmaktadır. Kriterlerin birbirlerine göre önem dereceleri belirlenirken Çizelge 4.20'de verilmiş olan ikili karşılaştırma matrisi şablonu esas alınmaktadır.

Çizelge 4.20. Örnek ikili karşılaştırma matrisi şablonu (Model adımı 3)

Kriterler (ikili karşılaştırma matrisi)	İşlem hacmi	Ağ gecikmesi	İşlem hızı	Olgunluk	Popülarite	Güvenilirlik	MoSCoW-S	MoSCoW-C	…
İşlem hacmi	1								
şAğ gecikmesi		1							
İşlem hızı			1						
Olgunluk				1					
Popülarite					1				
Güvenilirlik						1			
MoSCoW-S*							1		
MoSCoW-C**								1	
…									…

* Çizelge 4.18. MoSCoW listesinde "S" olarak seçilen kriter(ler)
** Çizelge 4.18. MoSCoW listesinde "C" olarak seçilen kriter(ler)

4.1.4. Adım 4. Hesaplama motoru

Toplanan bilgilerin belirlenmiş olan kurallara göre işleme sokularak somut çıktıların üretildiği, blokzincir çözümünün uygunluğu ve önerilen çözüm alternatiflerinin sıralamasının ortaya konulduğu aşamadır. Hesaplama motoru adımının girdileri, bu adımda gerçekleştirilen işlemler ve bu işlemler sonucunda elde edilen çıktılar alt başlıklar halinde aşağıda sıralanmaktadır.

Girdiler

İkinci ve üçüncü adımda hazırlanmış olan listeler ile üçüncü adımda temin edilen dış bilgi bu adımın girdilerini oluşturmakta olup aşağıdakileri içermektedir:

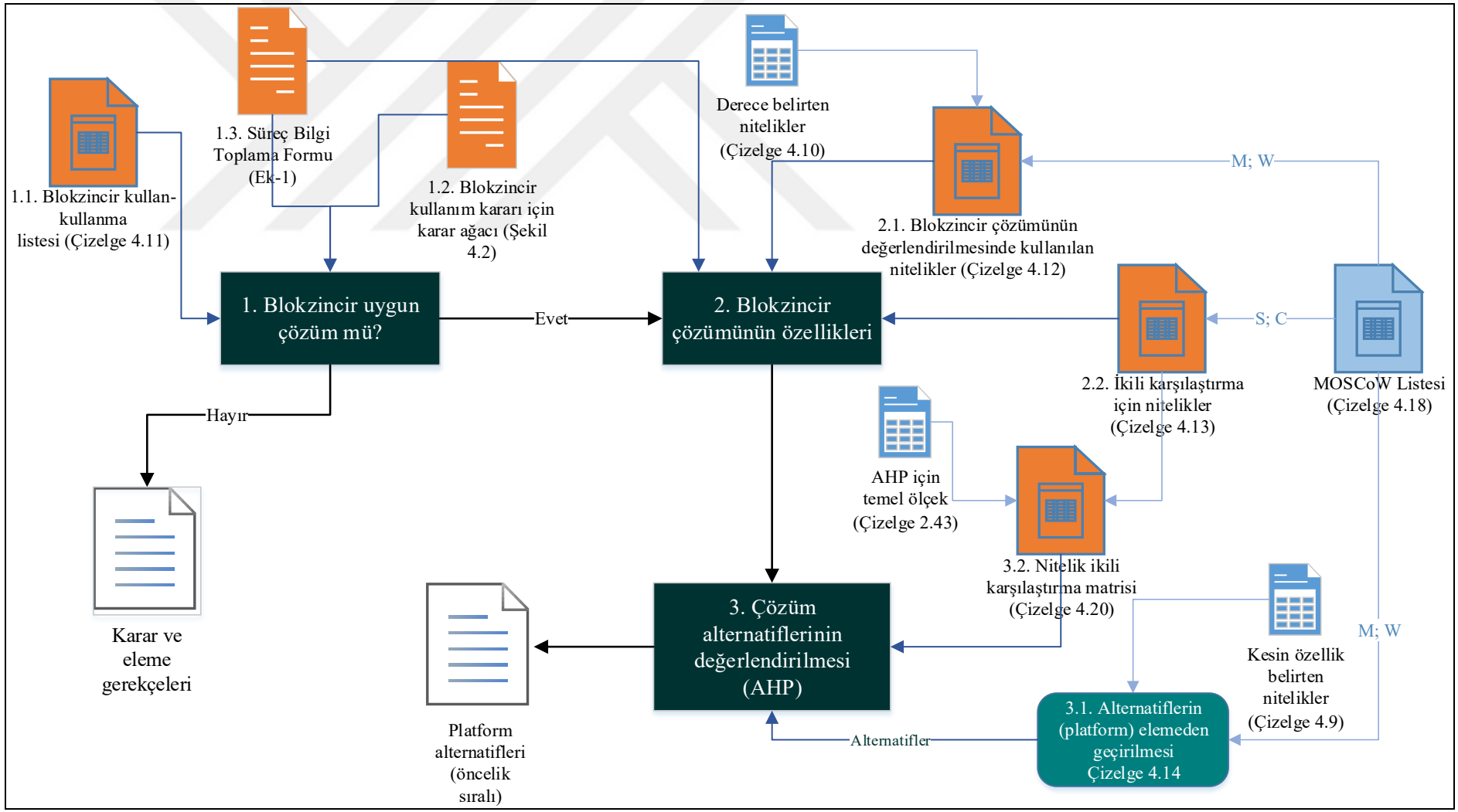
a) Blokzincir kullan-kullanma listesi (Çizelge 4.11)
b) Blokzincir kullanım kararı için karar ağacı (Şekil 4.2)
c) Platform karşılaştırma tablosu (Çizelge 4.7)
d) Süreç bilgileri
e) MoSCoW yanıt listesi (kullanıcı girişi)
f) Kriter önem sırası/derecesi (kullanıcı girişi)
g) İkili karşılaştırmalar için kriter listeleri (kullanıcı girişine göre hazırlanmaktadır)
h) Analitik Hiyerarşi Prosesi (AHP) işlem adımları

İşlemler

Modelin bu adımı daha önceki adımlarda derlenen, analiz edilen ve kullanıcıdan temin edilen veri ve bilgilerin işlendiği, takip eden adımlarda kullanılacak çıktıların üretildiği adımdır. Bu adımda temel olarak üç faaliyet gerçekleştirilmekte olup bu faaliyetler:

1. Blokzincir teknolojisinin seçilen süreç veya senaryo için uygun çözüm olup olmadığına karar verilmesi,
2. İstenen blokzincir çözümünün özelliklerinin, karar vermek için gerekli kriterlerin ve çözüm alternatiflerinin belirlenmesi,
3. Çözüm alternatiflerinin bu özelliklere göre değerlendirilerek öncelik sırasına göre sıralanması biçimindedir.

Bu faaliyetlerin detayları aşağıda sunulmakta olup ayrıca bir özeti Şekil 4.4'te verilmiştir.



Şekil 4.4. Adım 4. Hesaplama Motoru adımında gerçekleştirilen işlemler

Blokzincir teknolojisinin seçilen süreç veya senaryo için uygun çözüm olup olmadığına karar verilmesi

İlk aşamada süreç ya da kullanım senaryosu hakkında elde edilen bilgiler (Süreç Bilgi Toplama Formu) Çizelge 4.11'de verilmiş olan liste ile karşılaştırılarak blokzincirin uygun çözüm olup olmadığı kararı verilmektedir. Bu liste ile karşılaştırma sonucunda uygun çözüm olabileceği kararı verilmesi halinde Şekil 4.2'de verilmiş olan karar ağacı kullanılarak süreç/kullanım senaryosu yeni bir değerlendirmeye tabi tutulmaktadır.

Dördüncü adımın bu ilk faaliyeti yalnızca sonraki adımlara devam edilip edilmemesi kararına yardımcı olan, blokzincir çözümünün uygun olup olmadığ konusunda bir fikir veren ilk karar destek faaliyetidir.

Uygun blokzincir çözümünün özelliklerinin, karar vermek için gerekli kriterlerin ve çözüm alternatiflerinin belirlenmesi

Bu adımın ikinci faaliyeti son faaliyette gerçekleştirilecek kapsamlı hesaplamalar için gerekli girdilerin oluşturulmasını kapsamaktadır. Burada, öncelikle blokzincir çözümünden beklenen özellikler Çizelge 4.9'da verilmiş olan kesin özellik belirten nitelikler, Çizelge 4.18'de verilmiş olan MoSCoW listesinde "M" ve "W" olarak tercih edilmiş olan nitelikler ile birleştirilerek Çizelge 4.14'te yer verilmiş olan platform alternatifleri tablosunda uygun olmayan alternatifler elenmekte, AHP hesaplamalarında kullanılacak nihai alternatif listesi oluşturulmaktadır.

AHP hesaplamalarında kullanılacak diğer çıktı kriterler ve bu kriterlerin öncelikleridir. Bu kriterlerin listesi ise Çizelge 4.10'da verilmiş olan derece belirten niteliklere Çizelge 4.18'de verilmiş olan MoSCoW listesinde "S" ve "C" olarak seçilmiş olan niteliklerin eklenmesiyle oluşturulan Çizelge 4.13'te yer almaktadır. Çizelge 4.13'te yer alan kriterler Çizelge 2.41'de verilmiş olan AHP için temel ölçek kullanılarak birbirlerine göre öncelik değerlerinin belirlenmesi ve Çizelge 4.20'de verilmiş olan nitelik ikili karşılaştırma matrisinin hazırlanmasında kullanılmaktadır.

Özetle, dördüncü adımın bu faaliyetinde öncelikle mutlaka istenen ve kesinlikle istenmeyen özellikler dikkate alınarak uygun olmayan alternatifler elenip hesaplamalarda kullanılacak

nihai alternatif listesi oluşturulmaktadır. Daha sonra, çözüm alternatiflerinin karşılaştırılmasında kullanılacak kriterlere ilişkin matris, kullanıcı ve sürece göre önem derecelerine göre oluşturulmaktadır.

Çözüm alternatiflerinin bu özelliklere göre değerlendirilerek öncelik sırasına göre sıralanması

Bu adımın son faaliyetinde ise modelin temel çıktısı olan blokzincir çözümüne en uygun alternatiflerin öncelik sıralı listesini üretmek için Analitik Hiyerarşi Prosesi hesaplamaları gerçekleştirilmektedir. Bu hesaplamaların iki temel girdisi kriterler ve alternatifler olup önceki aşamalarda elde edilmiş olan bu girdiler kullanılarak Bölüm 2.7.3'te detaylı olarak anlatılmış olan AHP adımları uygulanmaktadır. Bu adımlar aşağıdaki biçimdedir:

1. Kriterler ve nihai alternatiflere göre blokzincir platform seçimi için hiyerarşi modelinin oluşturulması,
2. Blokzincir platform seçim kriterleri ikili karşılaştırma matrisinin hazırlanması (dördüncü adımın ikinci faaliyetinde hazırlanmaktadır),
3. İkili karşılaştırma matrisinin normalize edilmesi ve öncelik vektörünün hesaplanması,
4. Öncelik vektörü için tutarlılık analizinin gerçekleştirilmesi,
5. Her bir alternatifin her bir kritere göre birbirleriyle ikili karşılaştırma matrislerinin oluşturulması,
6. Alternatif ikili karşılaştırma matrislerinin normalize edilmesi (her bir kriter için ayrı ayrı),
7. Alternatif ikili karşılaştırma matrislerinin öncelik vektörünün hesaplanması (her bir kriter için ayrı ayrı),
8. Öncelik vektörleri için tutarlılık analizinin gerçekleştirilmesi (her bir kriter için ayrı ayrı),
9. Tüm kriterlere göre alternatiflerin ikili karşılaştırmaları sonucunda elde edilen ağırlık vektörleri kullanılarak alternatif-kriter matrisinin oluşturulması,
10. Alternatiflerin kriterlere göre ağırlıklarının matrisi ile seçim kriterlerinin ikili karşılaştırma matrisinden elde edilen ağırlık vektörünün çarpılması,
11. Onuncu maddedeki çarpım değeri sonuçlarının büyükten küçüğe sıralanarak alternatiflerin öncelik sırasının oluşturulması.

Yukarıda belirtilmiş olan tutarlılık analizi sonuçlarının eşik değeri aşması halinde ikili karşılaştırmalarda verilen öncelik değerleri yeniden değerlendirilerek işlemler tekrarlanmaktadır.

Çıktılar

Modelin sonraki aşamalarında kullanılmak üzere bu adımda elde edilmiş olan çıktılar aşağıdaki biçimdedir:

Blokzincir kullanım kararı

Blokzincir çözümünün kullanılmasının uygun bulunmaması halinde bu kararın gerekçeleri listelenmektedir.

Platform alternatifleri

Kullanıcı tarafından belirlenmiş olan öncelikler ve süreç özelliklerine göre uygun alternatifler AHP işlemleri sonucunda elde edilen puanları ile birlikte listelenmektedir.

4.1.5. Adım 5. Teknoloji seçimi ve sistem tasarımı

Bu adımda, dördüncü adımda elde edilen çıktılar, önceki adımlarda toplanmış ve üretilmiş olan bilgiler ile bir araya getirilerek uygun blokzincir çözümüne ilişkin mimari ortaya konulmaktadır.

Teknoloji seçimi ve sistem tasarımı adımının girdileri, bu adımda gerçekleştirilen işlemler ve bu işlemler sonucunda elde edilen çıktılar alt başlıklar halinde aşağıda sıralanmaktadır.

Girdiler

Önceki adımlarda nihai çıktı olarak elde edilmiş olan, doğrudan çözüm mimarisi için kullanılacak olan sonuç, liste ve bilgiler aşağıdakileri içermektedir:

a) Blokzincir kullanım kararı
   - Platform ve blokzincir fonksiyonel ve fonksiyonel olmayan özellikleri

b) Süreç bilgileri (gap analizi sonuçları)
    - Özellik listeleri (süreç teknik özellikleri ve performans özellikleri, süreçte rol alan taraflar ve rolleri)
c) MoSCoW yanıt listesi (Çizelge 4.18)
d) Öncelik sıralı kullanılabilir platform alternatifleri

İşlemler

Modelin bu adımında dördüncü adımda gerçekleştirilen hesaplama sonuçları birinci ve üçüncü adımlarda elde edilen çıktılarla derlenerek kullanıcıya sunulmak üzere hazırlanmaktadır. Bu adımda gerçekleştirilen faaliyetler aşağıdaki biçimdedir:

Sürecin blokzincir kullanımına uygun biçimde tasarlanması (Çizelge 4.15'te yer verilen konular)

İlk olarak, sürecin işlem adımları Süreç Bilgi Toplama Formu (Ek-1) ve bu formun çıktılarının Çizelge 4.15'te verilmiş olan kullanım alanlarına göre belirlenmektedir. İşlem adımları ve her bir adımda rol alan kurum/birimler listelendikten sonra sürecin akış şeması hazırlanmakta, sürecin yeni tasarıma göre özellikleri aşağıdakileri içerecek biçimde hazırlanmaktadır:

- Süreçte rol alan taraflar ve rolleri
- Süreç işlem hacmi (maksimum ve beklenen)
- Süreç işlem hızı
- Veri içeriği ve sınıflandırma (blok yapısı)
- Hassas, gizli ya da kritik veri ya da bilgi kullanımı
- Dış bilgi

Öncelik sırasına göre ilk sıradaki platformun teknik özelliklerinin listelenmesi

Tüm uygun alternatifler listelendikten sonra süreç için en uygun olduğu değerlendirilen platformun teknik özellikleri Çizelge 2.6'da verilmiş olan platform özellikleri şablonu esas alınarak aşağıdakileri içerecek biçimde hazırlanmaktadır:

- Blokzincir tipi

- Ağa katılım biçimi
- Kullanılan hash ve şifreleme algoritmaları
- Mutabakat mekanizması
- Yazılım dili ve tipi
- Performans özellikleri (işlem hacmi, ağ gecikmesi, işlem hızı, ölçeklenebilirlik)
- Güvenlik özellikleri (DDoS, Sybil saldırıları ve kuantum bilişime direnç)
- Akıllı sözleşme desteği ve detayları
- Platformun geliştiricisi, olgunluğu ve güvenilirliği

Çıktılar

Modelin son aşamasındaki raporlama için kullanılacak olan çıktılar aşağıdaki biçimdedir:

- Süreç (yeni) akış şeması (blokzincir teknolojisinin uygulandığı duruma göre)
- Yeni tasarlanan sürecin özellikleri
    - Süreç bilgileri
    - Blokzincir mimarisi
        - Blokzincir tipi
        - Ağ katılımcıları – düğümler ve rolleri
        - Blokzincirde kaydedilen işlemler
        - Blok yapısı
        - Sistemin güçlü ve zayıf yönleri
        - Blokzincir platformu

5. BLOKZİNCİR TEKNOLOJİSİNİN KULLANILABİLİRLİĞİ VE ÇÖZÜM SEÇİMİ İÇİN BİR UYGULAMA: KAMU İHALE SÜRECİ

Önerilen modelin uygulanabilirliğinin değerlendirilmesi, model işlem adımlarının uygulayıcılar için somutlaştırılması ve kavramsal model mimarisinin iyileştirilmesi amacıyla, seçilen bir süreç için modelin çalıştırılmasına karar verilmiştir.

Uygulama konusu seçilirken e-Devlet kapısında sunulan ve Bölüm 2.5.1'de detaylarına yer verilmiş olan hizmetler değerlendirilmiş, tüm kamu kurumlarında hemen hemen aynı işlem adımlarına sahip, genellikle aynı mevzuata tabi olan ve aşağıda verilmiş olan gerekçe ve problemli noktaları içeren kamu ihalelerinin gerçekleştirilmesi sürecinin uygulanmasına karar verilmiştir.

Uygulama alanı: Kamu İhale Süreci

Gerekçe: Tüm dünyada kamu ihaleleri sürecin belirli aşamalarındaki gizlilik ve güvenlik gereksinimi, değerlendirme ve sonuç aşamalarında da şeffaflık ve hesap verebilirlik ilkelerine uyum unsurları nedenleriyle en dikkat çeken kamu süreçlerinden biridir. Kamu harcamalarının en büyük kısmını oluşturan, ortak bir mevzuata tabi, içerisinde farklı görev, yetki, sorumluluk ve denetim rollerine sahip paydaşları bulunduran, çok aşamalı, nispeten karmaşık ve önemli mali ve itibari riskler barındıran bir süreç olması nedeniyle iyileştirmeye açık birçok alanı bulunmaktadır. Belediyeler, Üniversiteler, Genel ve Özel Bütçeli İdareler ile Kamu İktisadi Teşebbüslerini de içeren tüm Kamu Kurumlarında benzer sürecin uygulanıyor olması sürecin seçilmesinde dikkate alınan bir diğer unsurdur.

Mevcut Problemli Noktalar: Detaylarına modelin ilgili adımında yer verilmiş olmakla birlikte, kamu ihale sürecinin mevcut problemli noktaları aşağıdaki biçimdedir:

- Gizlilik ve güvenlik: hem ihale hem de teklif dokümanlarının gizliliği, güvenliği manuel kontrollere bağlıdır.
- Erişim kontrolleri: İhale dokümanlarına sadece yüklenici adaylarının erişim sağlaması, tekliflere sadece yetkilendirilmiş tarafların erişebilmesi, tüm erişimlerin kayıt altına alınabilmesi mevcut durumda fiziksel ve manuel kontrollere bağlıdır.

- Şeffaflık: Süreç içerisindeki işlem adımlarının ve değerlendirmelerin gerek kamuoyu gerekse diğer ilgili taraflar ve denetim görevlileri ile paylaşılması konusunda iyileştirilebilir-geliştirilebilir alanlar bulunmaktadır.
- Zaman: Mevcut durumda yazışmalar, ilan süreleri ve değerlendirme faaliyetleri için harcanan zamanda iyileştirilebilir-geliştirilebilir alanlar bulunmaktadır.

Blokzincirin Katacağı Değer: İhale sürecinde farklı rollere sahip tarafların oluşturduğu yönetişim yapısı mevcut durumda ihale sürecinin izlenmesini, güvenilirliğini ve şeffaflığını güçleştirmektedir. Süreçte yer alan ihaleyi düzenleyen kurum, yüklenici adayları, alt yüklenici ve tedarikçi adayları, teklifleri değerlendirmek üzere görevlendirilen heyet üyeleri (başka kurumdan temsilciler ve danışmanlar da dâhil), ihale sonucunu onaylayan makam gibi tarafların oluşturduğu yönetişim yapısı blokzincir teknolojisinden fayda sağlamak için oldukça uygundur. Blokzincir teknolojisinin bu süreçte kullanılmasının sağlayacağı faydalar şeffaflık, işlem hızı, güvenilirlik ve maliyet başlıkları altında değerlendirilmektedir.

Sürecin detayları ve blokzincir teknolojisinin bu süreçte kullanılabilirliğine ilişkin değerlendirme için önerilen modelin kullanımı her bir model adımı altında ayrı ayrı aşağıda detaylandırılmıştır.

5.1. Adım 1: Bilgi Tabanı

Modelin birinci adımı seçilen uygulama konusundan bağımsız olup ikinci adım olan "Kural Tabanı"na girdi sağlanan kısımdır. Ancak, uygulamanın gerçekleştirileceği döneme göre gözden geçirilerek gerekmesi halinde güncellemeler yapılarak bu güncellemeler doğrultusunda sonraki adımlardaki kurallar yeniden düzenlenebilmektedir. Olası değişiklik ve güncellemeler modelin işleyişinde bir değişiklik yaratmamaktadır. Bölüm 4.1.1'de verilmiş olan bu adımın içerdiği ve model kullanılmaya başlamadan önce gözden geçirilmesi önerilen konular aşağıda listelenmiştir:

- Blozkincir temel özellikler listesi (Çizelge 4.2)
- Avantajlar ve güçlü yönler listesi (Çizelge 4.4)
- Dezavantajlar ve zayıf yönler listesi (Çizelge 4.5)
- Blokzincir teknolojisinin hâlihazırda uygulanabilir olduğu süreçler (Çizelge 4.6)

- Blokzincir platformu karşılaştırma tablosu (Çizelge 4.7) – Bu tabloya aynı zamanda platform ilavesi de yapılabilmektedir.

5.2. Adım 2: Kural Tabanı

İkinci adım da birinci adımla aynı biçimde, seçilen uygulama konusundan bağımsız olarak hazırlanmış olan ve uygulama için aktif olarak kullanılmayan bir adımdır. Bu adımda, uygulama için kullanılacak kurallar bir defa oluşturulmuş olup ilk adımda yapılması muhtemel değişiklik ve güncellemeler doğrultusunda bu kuralların da hesaplama işlemleri öncesinde gözden geçirilmesi gerekmektedir. Herhangi bir değişiklik olmaması halinde ise dördüncü bölümde detayları verildiği biçimde aynen kullanılmaktadır.

Bölüm 4.1.2'de verilmiş olan bu adımın içerdiği ve model kullanılmaya başlamadan önce gözden geçirilmesi önerilen konular aşağıda listelenmiştir:

- Blokzincir platformunun niteliklerine ilişkin seçenekler - kesin özellik (Çizelge 4.9)
- Blokzincir platformunun niteliklerine ilişkin seçenekler - derece belirten (Çizelge 4.10)
- Blokzincir kullan-kullanma listesi (Çizelge 4.11)
- Blokzincir kullanım kararı için karar ağacı (Şekil 4.2)
- MoSCoW özellik listesi (Çizelge 4.12)
- Blokzincir platformları için ikili karşılaştırma nitelikleri (Çizelge 4.13)
- MoSCoW listesine göre platform değerlendirme tablosu (Çizelge 4.14)

5.3. Adım 3. Süreç Seçimi, Bilgi Toplama ve Veri Girişi

Bu adımda, seçilen kamu ihale süreci için bilgiler toplanarak kullanıcı veri girişi sağlanmaktadır. Bu bilgilerin sistematik bir biçimde toplanması için Ek-1'de verilmiş olan Süreç Bilgi Toplama Formu kullanılmaktadır. Edinilen bilgilerden MoSCoW özellik listesinin seçilen sürece uygun biçimde hazırlanması ve ikili karşılaştırmalar için kriter listesinin hazırlanmasında faydalanılmaktadır.

Buna göre, Ek-1'de şablonu verilmiş olan form, Kamu İhale Süreci için doldurularak Ek-2'de verilmiş olup bu formda yer verilen bilgiler modelin sonraki adımlarında kullanılmak üzere aşağıda özetlenmiştir:

1. Kullanım senaryosu, birden fazla kurumu/birimi içeren bir iş ağını kapsıyor mı?

   ◉ Evet
   ○ Hayir

2. Süreç işlem hacmi, önceki yıllara ait değerler (işlem adedine göre, yılda işlem sayısı) aşağıdaki biçimdedir.

Çizelge 5.1. İhale süreci işlem hacmi (yıl/ihale sayısı)

	2011	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**
İhale sayısı	213 587	141 731	175 724	157 879	164 327	160 437	135 260	112 446	95 109	100 350	86 711
İdare sayısı	15 914	11 944	12 960	12 974	12 211	12 299	12 283	10 769	9 524	8 923	9 053
Ort	14	12	14	13	14	14	12	11	10	12	10

Buna göre, 2011 2021 yılları arasında idare başına düşen ortalama ihale sayılarının ortalaması da 11,8'dir.

3. Süreç tarafından üretilen/depolanan veri miktarı (tahmini ya da ölçüm değeri): Süreç içerisinde üretilen ve depolanan veri miktarı değişken olmakla birlikte bu veri miktarının yıllık bir gb'ı aşmayacağı öngörülmektedir. Ancak, bu verinin blokzincirde tutulmaması, sadece verinin hash değeri ile işlem yapılması halinde bu veri boyutu çok daha düşük olacaktır.

4. Süreç işlem hızı (mevcut/istenen/max/min) ve anlık doğrulama: Süreç işlem hızı belirsiz ve değişken olup seçilen süreç için kritik bir performans göstergesi değildir. İşlemler için anlık doğrulama gerekmemektedir.

5. Blokzincir üçlü açmazı (ölçeklenebilirlik, merkezsizlik ve güvenlik): Kamu ihale süreci için en önemli özellik güvenliktir. Süreç bir kamu kurumu tarafından sunulan bir hizmet olduğundan merkezsizlik en az öneme sahip özelliktir.

6. Süreç veri içeriği: Süreç veri içeriği kısmında hazırlanmış olan bilgilere ilişkin detaylar Ek-2'de verilmiş olup doğrudan modelin beşinci adımında kullanılacaktır.

7. Veri sınıflandırma: Veri sınıflandırma kısmında hazırlanmış olan bilgilere ilişkin detaylar Ek-2'de verilmiş olup doğrudan modelin beşinci adımında kullanılacaktır.

8. Sürecin işleyişi: Sürecin işleyişi kısmında hazırlanmış olan akış şeması ve açıklamalara ilişkin detaylar Ek-2'de verilmiş olup doğrudan modelin beşinci adımında kullanılacaktır.

9. Hassas, gizli ya da kritik bilgi ya da veri kullanımı: Süreç içerisinde hazırlanan ve kullanılan veri ve bilgilere ilişkin detaylar Ek-2'de verilmiş olup doğrudan modelin beşinci adımında kullanılacaktır.

10. Dış bilgi gereksinimi: Süreç içerisinde kullanılan banka dekontu, geçici teminat mektubu, yetki belgesi gibi dış dokümanların tamamı teklif paketi içerisinde değerlendirilmektedir.

11. Mevcut mevzuat: Örnek uygulama için bir kamu kurumunun kalite dokümanlarında tanımlı kurum içi Süreç Tanımı kısmen esas alınmıştır.

12. Fonksiyonel gereksinimler: Sistemin gerçekleştirmesi istenen özelliklerin detayları Ek-2'de verilmiş olup bunlar; ortak ve tutarlı veri saklama, birden fazla kullanıcının kayıt yazabilmesi, tüm kayıt ekleyebilen aktörler arasında güven ve hiyerarşi eksikliği, kayıtların değiştirilememesi, silinememesi, güncellenememesi, katılımcıların belirlenen düzeyde anonimliğe sahip olması biçimindedir. Fonksiyonel özelliklerden biri olan "aracı ya da merkezi otorite bulunmaması" seçilen süreç için aranan bir özellik değildir.

13. Fonksiyonel olmayan gereksinimler: Sistemin kalite özelliklerini tanımlayan gereksinimler ve süreç için kritiklikleri aşağıda sıralanmaktadır.
    - Ölçeklenebilirlik: Düşük
    - İşlem hızı: Düşük
    - İşlem hacmi: Düşük
    - Sistem güvenliği (çatallanma, mutabakat mekanizması açıkları): Yüksek
    - Diğer sistemlerle entegrasyon: Orta

- Verimlilik: Orta
- Mevzuat düzenlemelerine uyum: Yüksek
- Teknik ve süreç olgunluk/ standardizasyon düzeyi: Orta
- Şeffaflık: Yüksek

14. Mevcut süreç/faaliyetle ilgili problemler ya da iyileştirilebilir noktalar: Detayları Ek-2'de verilmiş olup blokzincir teknolojisinden faydalanılabilecek iyileştirilebilir alanlar gizlilik ve güvenlik, erişim kontrolleri, şeffaflık, sürecin tamamlanması için geçen zaman ve tarih kontrolü başlıkları altında toplanmıştır.

Toplanan bu bilgiler doğrultusunda, modelin bir sonraki adımında kullanılmak üzere Çizelge 4.9'da verilmiş olan blokzincir platformunun niteliklerine ilişkin seçenekler (kesin özellik) tablosu, ardından Çizelge 4.10'da verilmiş olan blokzincir platformunun niteliklerine ilişkin seçenekler (derece belirten) tablosu kullanıcı tercihleri ve beklenen özellikler doğrultusunda doldurulmaktadır. Buna göre, kesin özellikler Çizelge 5.2'de, derece belirten özellikler ise Çizelge 5.3'te verilmiştir.

Çizelge 5.2. Blokzincir platformunun kesin niteliklerine ilişkin seçenekler (ihale süreci)

Nitelik	Seçim zorunlu mu?	Seçenekler	Karar
Ağa katılım	Opsiyonel	**İzin gerektiren (1)**, İzin gerektirmeyen (2), Her iki tipte de konfigüre edilebilir (3)	1
Blokzincir tipi (açık, özel)	Opsiyonel	Açık (1), **Özel (2)**, Her iki tipte de konfigüre edilebilir (3)	2
Yazılım tipi (açık kaynak kodlu, lisanslı)	Opsiyonel	Açık kaynak kodlu (1), lisanslı (2), kendi bünyesinde geliştirme (3), diğer (4)	Hepsi
Uygulama türü	Zorunlu	Genel amaçlı (1), **Sadece belirli işlemler için (2)**	2
Akıllı sözleşme desteği	Opsiyonel	**Evet (1)**, Hayır (2)	1
Token kullanımı	Opsiyonel	Evet (1), Hayır (2)	Hepsi

Çizelge 5.3. Blokzincir platformunun derece belirten niteliklerine ilişkin seçenekler (ihale süreci)

Nitelik	Seçim zorunlu mu?	Seçenekler	Karar
İşlem hacmi (saniyede işlem sayısı)	Opsiyonel	**Çok düşük (1)**, Düşük (2), Orta (3), Yüksek (4), Çok yüksek (5)	1
Ağ gecikmesi	Opsiyonel	Çok düşük (1), Düşük (2), **Orta (3), Yüksek (4)**, Çok yüksek (5)	3, 4
Ölçeklenebilirlik	Opsiyonel	Çok düşük (1), **Düşük (2), Orta (3)**, Yüksek (4), Çok yüksek (5)	2, 3
İşlem hızı	Opsiyonel	**Çok düşük (1), Düşük (2)**, Orta (3), Yüksek (4), Çok yüksek (5)	1, 2

Blokzincir üçlü çelişkisi (ölçeklenebilirlik, güvenlik, merkezsizlik)	Hangisinden feragat edilebileceği seçilecektir	**(1) Merkezsizlik** (2) Ölçeklenebilirlik (3) Güvenlik ( ) Hiçbiri	1
DoS ve DDoS saldırılarına direnç	Opsiyonel	Düşük (1), Orta (2), **Yüksek (3)**	3
Sybil saldırısına direnç	Opsiyonel	Düşük (1), Orta (2), **Yüksek (3)**	3
Kuantum bilişim riskine direnç	Opsiyonel	Düşük (1), Orta (2), **Yüksek (3)**	3
Mahremiyet ve gizlilik teknolojisi	Opsiyonel	**Düşük (1)**, Orta (2), Yüksek (3)	1
Olgunluk	Opsiyonel	Çok düşük (1), Düşük (2), Orta (3), **Yüksek (4), Çok yüksek (5)**	4, 5
Pazardaki popülarite	Opsiyonel	Çok düşük (1), Düşük (2), Orta (3), **Yüksek (4), Çok yüksek (5)**	4, 5
Güvenilirlik	Opsiyonel	Çok düşük (1), Düşük (2), Orta (3), **Yüksek (4), Çok yüksek (5)**	4, 5

Bu bilgilere göre, yine modelin hesaplama adımında kullanılmak üzere hazırlanan seçim listesi MoSCoW metodu için Çizelge 5.4'te verilmiştir.

Çizelge 5.4. MoSCoW– önceliklerin belirlenmesi için kullanılan seçim listesi (ihale süreci)

Nitelik Grubu	**Nitelik**	**Seçenek (MoSCoW)**			
		M	**S**	**C**	**W**
Ağa katılım	İzin gerektiren	✓			
	İzin gerektirmeyen				✓
	Her iki tipte de konfigüre edilebilir				
Blokzincir tipi (açık, özel)	Açık blokzincir				✓
	Özel blokzincir	✓			
	Her iki tipte de konfigüre edilebilir				
Yazılım tipi	Açık kaynak kodlu				
	Lisanslı				
	Kendi bünyesinde geliştirme				
Güvenlik	DoS ve DDoS saldırılarına direnç			✓	
	Sybil saldırısına direnç			✓	
	Kuantum bilişime direnç			✓	
	Akıllı sözleşme desteği	✓			
	Token kullanımı			✓	
Blokzincir üçlü çelişkisi	Ölçeklenebilirlik				
	Güvenlik	✓			
	Merkezsizlik				

MoSCoW seçimleri de yapıldıktan sonra "S" (olması faydalı olanlar) ve "C" (olması iyi karşılananlar) olarak seçilen nitelikler Çizelge 4.13'te verilmiş olan blokzincir platformları için ikili karşılaştırma nitelikleri tablosuna eklenerek nihai ikili karşılaştırma nitelik tablosu oluşturulmaktadır. Oluşturulan bu tablo Çizelge 5.5'te verilmiştir.

Çizelge 5.5. Blokzincir platformları için ikili karşılaştırma nitelikleri (ihale süreci)

Nitelik Grubu	Nitelik	Seçenek
~~Güvenlik (opsiyonel)~~	~~Mahremiyet ve gizlilik teknolojisi*~~	~~Düşük~~
Performans	İşlem hacmi	Çok düşük
	Ağ gecikmesi	Orta
	İşlem hızı	Düşük
Diğer	Olgunluk	Çok yüksek
	Popülarite	Çok yüksek
	Güvenilirlik	Çok yüksek
MoSCoW tablosu	DoS ve DDoS saldırılarına direnç	C
	Sybil saldırısına direnç	C
	Kuantum bilişime direnç	C
	Token kullanımı	C
** Tüm platform alternatifleri için değeri "3" olduğundan kriter olarak kullanılmasına gerek bulunmamaktadır.*		

Bu adımda son olarak kriterlerin birbirlerine göre önem derecelerinin belirlenmesi işlemi gerçekleştirilmektedir. Bu işlem, Çizelge 5.5'te verilmiş olan nihai kriterlerin, Çizelge 2.41'de verilmiş olan AHP için temel ölçek tablosundaki "mutlak ölçekte önem kuvveti" değerleri kullanılarak birbirlerine göre önem derecelerinin belirlenmesini içermektedir.

İkili karşılaştırma niteliklerine göre, platform seçiminde değerlendirilecek kriter sayısı 10'dur. Bu kriterler; İşlem hacmi, ağ gecikmesi, işlem hızı, olgunluk, popülarite, güvenilirlik, DoS ve DDoS saldırılarına direnç, Sybil saldırısına direnç, Kuantum bilişime direnç ve token kullanımıdır. Bu kriterlerin birbirlerine göre önem dereceleri kullanıcıdan alınan bilgiler doğrultusunda, Ek-1 Süreç Bilgi Formundan faydalanılarak hazırlanan aşağıdaki ifadelere göre belirlenmektedir:

- Kriterlerin birbirlerine göre önem dereceleri belirlenmeden önce, öncelikle önem dereceleri eşit olan kriterler belirlenmektedir. Buna göre performans özellikleri olan "Ağ gecikmesi", "İşlem hacmi" ve "İşlem hızının" önem dereceleri birbirlerine eşittir.
- Güvenlik özellikleri olan DoS ve DDoS saldırılarına direnç, Sybil saldırısına direnç, Kuantum bilişime direnç için önem sıralaması Sybil > Kuantum > DDoS biçimindedir.
- Diğer özellikler başlığı altındaki Güvenilirlik, Olgunluk ve Popülarite kriterlerinin önem sıralaması Güvenilirlik > Olgunluk > Popülarite biçimindedir. Platform alternatifleri için en önemli kriter grubu "Diğer" başlığı altındaki bu üç kriterdir.
- İkinci derecede öneme sahip kriter grubu "Güvenlik", üçüncü derecede öneme sahip kriter grubu ise "Performans"tır.

- Henüz yasal düzenlemesi bulunmayan, kamu hizmetlerinde kullanılması yakın gelecekte beklenmeyen "Token kullanımı" kriteri en düşük önemdeki kriterdir.
- Kriterlerin önem sıralaması; "Güvenilirlik > Olgunluk > Popülarite > Sybil > Kuantum > DDoS > Ağ gecikmesi = İşlem hacmi = İşlem hızı > Token kullanımı" biçiminde olup kriterlerin birbirlerine göre önem dereceleri aşağıdaki biçimdedir[9]:
  - Güvenilirlik:
    - Olgunluk kriterine göre biraz daha önemli (3),
    - Popülarite kriterine göre biraz daha fazla önemli (4),
    - Sybil saldırılarına direnç kriterine göre esaslı veya güçlü önemde (5),
    - Kuantum saldırılarına direnç kriterine göre esaslı veya güçlü önem ile çok güçlü önem arasında (6),
    - DoS ve DDoS saldırılarına direnç kriterine göre çok güçlü önemde (7),
    - Ağ gecikmesi, işlem hacmi ve işlem hızı kriterlerine göre çok güçlü ile son derece önemli arasında (8),
    - Token kullanımı kriterine göre ise son derece önemlidir (9).
  - Olgunluk
    - Popülarite kriterine göre biraz daha önemli (2),
    - Sybil saldırılarına direnç kriterine göre biraz daha önemli (3),
    - Kuantum saldırılarına direnç kriterine göre esaslı veya güçlü önem ile biraz daha önemli arasında (4),
    - DoS ve DDoS saldırılarına direnç kriterine göre esaslı veya güçlü önemde (5),
    - Ağ gecikmesi, işlem hacmi ve işlem hızı kriterlerine göre esaslı veya güçlü önem ile çok güçlü önem arasında (6),
    - Token kullanımı kriterine göre ise çok güçlü önem ile son derece önemli arasındadır (8).
  - Popülarite
    - Sybil saldırılarına direnç kriterine göre biraz daha önemli (2),
    - Kuantum saldırılarına direnç kriterine göre biraz daha önemli (3),
    - DoS ve DDoS saldırılarına direnç kriterine göre esaslı veya güçlü önem ile biraz daha önemli arasında (4),

[9] Önem derecelerine ilişkin ifadelerin sonunda parantez içinde yer verilmiş olan değerler Çizelge 2.41 AHP için temel ölçek esas alınarak belirlenmiş olan önem derecesini ifade etmektedir.

- Ağ gecikmesi, işlem hacmi ve işlem hızı kriterlerine göre esaslı veya güçlü önemde (5),
- Token kullanımı kriterine göre ise çok güçlü önemdedir (7).

o Sybil saldırılarına direnç
- Kuantum saldırılarına direnç kriterine göre biraz daha önemli (2),
- DoS ve DDoS saldırılarına direnç kriterine göre biraz daha önemli (3),
- Ağ gecikmesi, işlem hacmi ve işlem hızı kriterlerine göre esaslı veya güçlü önem ile biraz daha önemli arasında (4),
- Token kullanımı kriterine göre ise esaslı veya güçlü önem ile çok güçlü önem arasındadır (6).

o Kuantum saldırılarına direnç
- DoS ve DDoS saldırılarına direnç kriterine göre biraz daha önemli (2),
- Ağ gecikmesi, işlem hacmi ve işlem hızı kriterlerine göre biraz daha önemli (3),
- Token kullanımı kriterine göre ise esaslı veya güçlü önemdedir (5).

o DoS ve DDoS saldırılarına direnç
- Ağ gecikmesi, işlem hacmi ve işlem hızı kriterlerine göre biraz daha önemli (2),
- Token kullanımı kriterine göre ise esaslı veya güçlü önem ile biraz daha önemli arasındadır (4).

o Ağ gecikmesi, işlem hacmi ve işlem hızı
- Token kullanımı kriterine göre biraz daha önemlidir (3).

Kriterlerin birbirlerine göre önem derecelerine ilişkin değerlendirmeler ve bu değerlendirmeler doğrultusunda belirlenen önem derecelerine göre hazırlanmış olan matris Çizelge 5.6'da verilmiştir.

Çizelge 5.6. Seçim kriterlerinin birbirlerine göre önem dereceleri (ihale süreci)

Kriterler (ikili karşılaştırma matrisi)	Güvenilirlik	Olgunluk	Popülarite	Sybil direnci	Kuantum direnci	DoS& DDoS direnci	Ağ gecikmesi	İşlem hacmi	İşlem hızı	Token kullanımı
Güvenilirlik	1	3	4	5	6	7	8	8	8	9
Olgunluk	1/3	1	2	3	4	5	6	6	6	8
Popülarite	1/4	1/2	1	2	3	4	5	5	5	7
Sybil direnci	1/5	1/3	1/2	1	2	3	4	4	4	6
Kuantum direnci	1/6	1/4	1/3	1/2	1	2	3	3	3	5
DoS& DDoS direnci	1/7	1/5	1/4	1/3	1/2	1	2	2	2	4
Ağ gecikmesi	1/8	1/6	1/5	1/4	1/3	0,500	1	1	1	3

İşlem hacmi	1/8	1/6	1/5	1/4	1/3	0,500	1	1	1	3
İşlem hızı	1/8	1/6	1/5	1/4	1/3	0,500	1	1	1	3
Token kullanımı	1/9	1/8	1/7	1/6	1/5	0,250	1/3	1/3	1/3	1
Çizelge 5.6'da verilmiş olan matriste önem dereceleri belirlenirken AHP için temel ölçekten (Bkz. Çizelge 2.41) faydalanılmıştır.										

5.4. Adım 4. Hesaplama Motoru

Önceki adımlarda oluşturulan listeler ve girdiler kullanılarak blokzincir çözümünün kamu ihale sürecine uygun olup olmadığı değerlendirilmekte, uygun olması halinde çözüm için uygun blokzincir platform alternatifleri listelenmektedir. Bu adımda gerçekleştirilen işlemler ve hesaplamalar aşağıda verilmiştir.

5.4.1. Blokzincir teknolojisinin seçilen süreç veya senaryo için uygun çözüm olup olmadığına karar verilmesi

İlk olarak blokzincir kullan-kullanma listesi (Bkz. Çizelge 4.11) kullanılarak kamu ihale sürecinin bu listede yer alıp almadığı kontrol edilmektedir. Çizelge 4.11 kullanılarak kamu ihale süreci için blokzincir teknolojisinin kullanımına ilişkin yapılan değerlendirme Çizelge 5.7'de verilmiştir.

Çizelge 5.7. Hâlihazırdaki blokzincir kullanım alanlarına göre ihale sürecinin değerlendirilmesi

Soru	Seçenekler	Yanıt	Değerlendirme
Kullanım senaryosu şunlardan birini içeriyor mu?*	Dijital kimlik yönetimi Dijital sertifika (diploma, transkript, eğitim belgesi vb.) Elektronik oylama Gayrimenkul kayıt sistemi Ürün takibi (gıda, ilaç vb.) **İhale ve satınalma sistemi** İzlenebilirlik ve orijinallik kontrolü Kişisel kayıtların yönetimi (sağlık, finans vb.) Mesajlaşma sistemi Noter onayı Sosyal yardımların dağıtılması Tedarik zinciri yönetimi Telif hakları yönetimi	Evet	Blokzincirin hâlihazırda uygulanabilir olduğu süreçlerden biridir. İlk aşama kullan/kullanma kararı verilmesine gerek duyulmadan doğrudan platform değerlendirme adımlarına geçilebilir.
Kullanım senaryosu şunlardan en az birini gerektiriyor mu?	Çok yüksek veri hacmi, Çok yüksek işlem hızı, Çok yüksek işlem sayısı, Yüksek performans, Veri silme, değiştirme ya da güncelleme	Hayır	Evet ise açık blokzincir kullanımı önerilmez

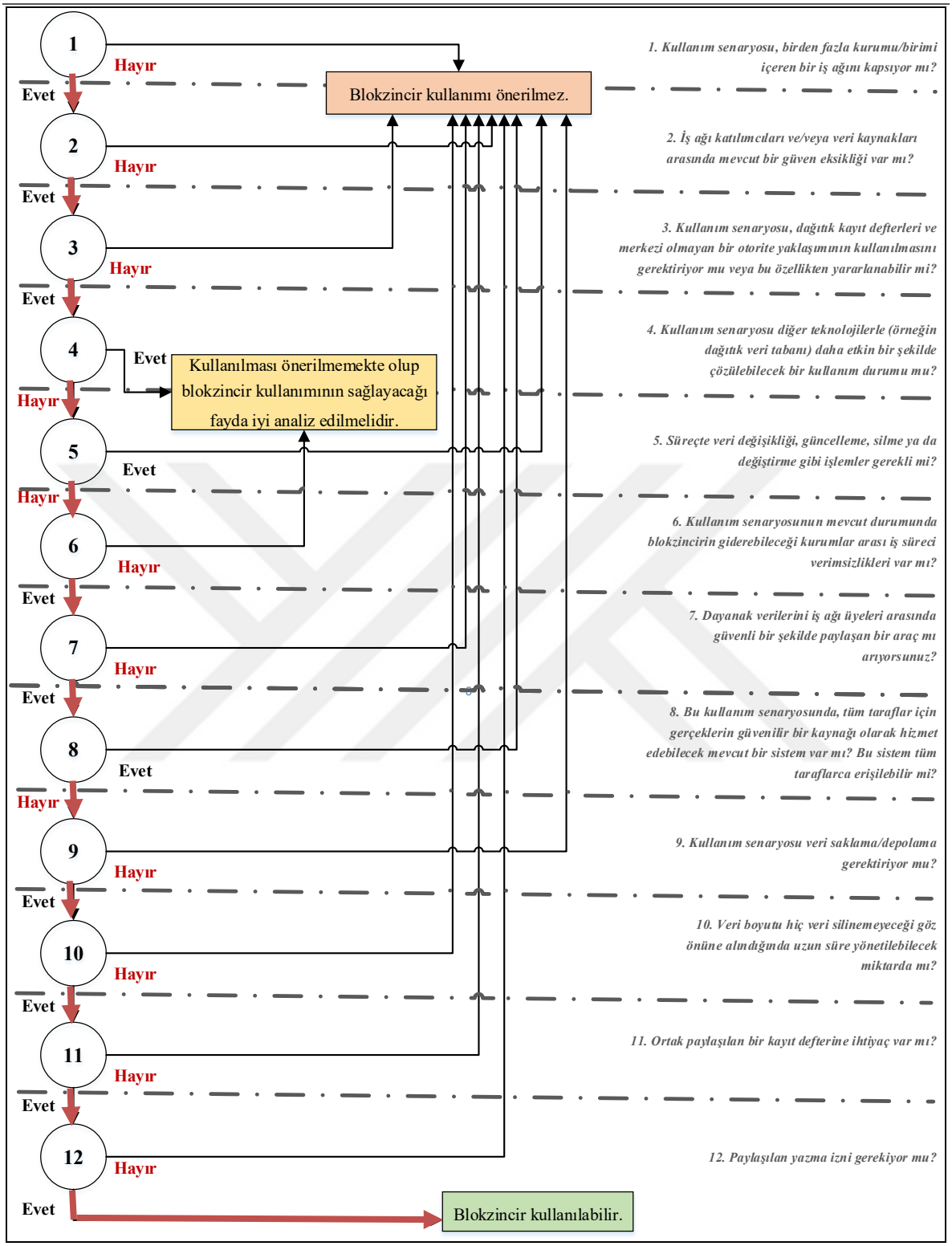
Bu yanıtlara göre, ihale işlemleri süreci blokzincirin uygulanabilir olduğu süreçlerden biridir. Bu durumda, doğrudan blokzincirin kullanılabilir olduğu kararı ile platform değerlendirme aşamasına geçilebilir. Ancak, burada, modelin ilk adımındaki işlemlerin doğrulanması için karar ağacı ve ilk aşama kararı için hazırlanmış olan soruların değerlendirilmesi işlemleri gerçekleştirilmektedir.

Blokzincir kullanım kararı için karar ağacının kullanımına yönelik cevaplar Çizelge 5.8'de verilmiştir.

Çizelge 5.8. Blokzincir kullanım kararı karar ağacı soru ve yanıtları (ihale süreci)

	Soru	Yanıt (Kamu İhale Süreci Bilgi Formu)	Evet	Hayır
1	Kullanım senaryosu, birden fazla kurumu/birimi içeren bir iş ağını kapsıyor mı?	*Evet (Form, Soru 1)*	**Blokzincir kullanılabilir.**	Blokzincir kullanımı önerilmez.
2	İş ağı katılımcıları ve/veya veri kaynakları arasında mevcut bir güven eksikliği var mı?	*Evet*	**Blokzincir kullanılabilir.**	Blokzincir kullanımı önerilmez.
3	Kullanım senaryosu, dağıtık kayıt defterleri ve merkezi olmayan bir otorite yaklaşımının kullanılmasını gerektiriyor mu veya bu özellikten yararlanabilir mi?	*Evet (Form, Soru 12)*	**Blokzincir kullanılabilir.**	Blokzincir kullanımı önerilmez.
4	Kullanım senaryosu diğer teknolojilerle (örneğin dağıtık veri tabanı) daha etkin bir şekilde çözülebilecek bir kullanım durumu mu?	*Hayır* *Klasik veritabanı ya da dağıtık veritabanı çözümleri ile süreç işletilebilse de, blokzincirin sağladığı şeffaflık ve değiştirilemezlik özellikleri bu süreç için blokzincir teknolojisini avantajlı kılmaktadır.*	Kullanılması önerilmemekte olup blokzincir kullanımının sağlayacağı fayda iyi analiz edilmelidir.	**Blokzincir kullanılabilir.**
5	Kullanım durumu katı biçimde işlem değişmezliği gerektiriyor mu veya bu özellikten yararlanabilir mi? *Süreçte veri değişikliği, güncelleme, silme ya da değiştirme gibi işlemler gerekli mi?*	*Hayır (Form, Soru 12)*	Blokzincir kullanılamaz	Blokzincir kullanılabilir.
6	Kullanım senaryosunun mevcut durumunda kurumlar arası iş süreci verimsizlikleri var mı? Blokzincirin kendisine has özellikleri bu verimsizlikleri giderebilir mi?	*Evet (Form, Soru 14)*	**Blokzincir kullanılabilir.**	Kullanılması önerilmemekle birlikte blokzincir kullanımının sağlayacağı fayda iyi analiz edilmelidir.
7	Dayanak verilerini iş ağı üyeleri arasında güvenli bir şekilde paylaşan bir araç mı arıyorsunuz?	*Evet (Form, Soru 14)*	**Blokzincir kullanılabilir.**	Blokzincir kullanımı önerilmez.
8	Bu kullanım senaryosunda, tüm taraflar için gerçeklerin güvenilir bir kaynağı olarak hizmet edebilecek mevcut bir sistem var mı? Bu sistem tüm taraflarca erişilebilir mi? (Sürekli çevrimiçi güvenilir bir üçüncü taraf kullanılıyor mu?)	*Hayır (Form, Soru 8)* *(Süreçte basılı kâğıt ortamında ihale dokümanları güvenilir veri kaynağı olarak tutulmakta ve sunulmaktadır. Tüm taraflar bu verilere açık biçimde ulaşamamaktadır)*	Blokzincir kullanımı önerilmez.	**Blokzincir kullanılabilir.**
9	Kullanım senaryosu veri saklama/depolama gerektiriyor mu?	*Evet (Form, Soru 8)*	**Blokzincir kullanılabilir.**	Blokzincir kullanımı önerilmez.
10	Veri boyutu hiç veri silinemeyeceği göz önüne alındığında uzun süre yönetilebilecek miktarda mı?	*Evet (Form, Soru 6)*	**Blokzincir kullanılabilir.**	Blokzincir kullanımı önerilmez.
11	Ortak paylaşılan bir kayıt defterine ihtiyaç var mı?	*Evet (Form, Soru 12)*	**Blokzincir kullanılabilir.**	Blokzincir kullanımı önerilmez.
12	Paylaşılan yazma izni gerekiyor mu?	*Evet (Form, Soru 12)*	**Blokzincir kullanılabilir.**	Blokzincir kullanımı önerilmez.

Verilen yanıtlara göre oluşturulan karar ağacı Şekil 5.1'de verilmiştir.



Şekil 5.1. Kamu İhale Süreci için blokzincir kullanımı karar ağacı

Karar ağacında yer alan 12 soruya verilen yanıtlar doğrultusunda ilk karar aşamasında, süreç için blokzincirin kullanılabilir olduğu sonucuna ulaşılmıştır.

5.4.2. Uygun blokzincir çözümünün özelliklerinin, karar vermek için gerekli kriterlerin ve çözüm alternatiflerinin belirlenmesi

Blokzincir teknolojisinin kamu ihale süreci için kullanılabilir olduğu değerlendirmesinden sonra, uygun blokzincir çözümüne karar vermek için değerlendirme kriterleri ve çözüm alternatifleri ortaya konmakta, alternatifler, bu kriterler dikkate alınarak ve birbirleri ile karşılaştırılarak en uygun seçenek tespit edilmektedir.

Bunun için, öncelikle, Çizelge 5.4'te verilmiş olan MoSCoW seçim listesinde mutlaka olması ve kesinlikle bulunmaması istenen özelliklere göre platform alternatifleri değerlendirilerek ilk eleme işlemi gerçekleştirilmektedir. Bu değerlendirmeler aşağıdaki biçimdedir:

- Ağa katılım:
  - İzin gerektiren olması (M) istenmektedir. Bu durumda, "1" izin gerektiren ya da "3" her iki tipte de konfigüre edilebilir olan platformlar seçilecektir.
  - İzin gerektirmeyen olmaması (W) istenmektedir. Bu durumda "2" izin gerektirmeyen olan platformlar elenecektir. İlk soruya göre yapılan değerlendirme ile aynı sonucu verdiğinden bu satırın doldurulmasına gerek bulunmamaktadır.
- Blokzincir tipi:
  - Özel blokzincir olması istenmektedir (M). Bu durumda, özel (2) ya da her iki tipte de konfigüre edilebilir (3) platformlar seçilecek, diğerleri elenecektir.
- Yazılım tipi ve güvenlik özellikleri için tercih belirtilmemiştir. Bu durumda tüm platform alternatifleri seçilebilirdir.
- Akıllı sözleşme
  - Akıllı sözleşme desteği istenmektedir (M). Bu durumda, akıllı sözleşme desteği sunan (1) platformlar seçilecek, diğerleri elenecektir.
- Güvenlik:
  - Ölçeklenebilirlik, güvenlik ve merkezsizlik bir arada değerlendirilmekte olup uygulama olarak seçilen süreçte feragat edilebilecek özellik merkezsizlik olarak ifade edilmektedir. Bu durumda, referans tabloda blokzincir üçlü çelişkisi (ölçeklenebilirlik, güvenlik, merkezsizlik) olarak belirtilmiş satır için, "Ölçeklenebilir ve güvenli ama merkezi (1)" özelliğini taşıyan platformlar seçilecek,

diğerleri elenecektir. Burada, Avalanche ve Kadena üç özelliği de sağlayan platformlar olduğu için (4) bu platformlar da seçime dâhil edilmiştir.

Tercih belirtilmiş olan dört özellik için bu değerler girildikten sonra, her bir özellik için "1" yani "evet" değerini taşıyan platform alternatifleri seçilir. Yukarıda verilen açıklamalar doğrultusunda hazırlanmış olan platform değerlendirme tablosu Çizelge 5.9'da verilmiştir.

Çizelge 5.9. MoSCoW listesine göre platform değerlendirme tablosu

		Seçim (0, 1)	M/W	Bitcoin	Ethereum	Hyperledger	Stellar	Quorum	Corda	Multichain	OpenChain	BigchainDB	IOTA	HydraChain	Avalanche	Parity	Kadena
Ağa katılım	İzin gerektiren	1	M	0	0	1	0	1	1	1	1	1	1	1	1	1	1
	İzin gerektirmeyen	0	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	Her iki tipte de konfigüre edilebilir	0	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Blokzincir tipi	Açık blokzincir	1	W	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	Özel blokzincir	1	M	0	0	1	0	1	1	1	1	1	1	1	1	1	1
	Her iki tipte de konfigüre edilebilir	0	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Yazılım tipi	Açık kaynak kodlu	0	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	Lisanslı	0	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	Kendi bünyesinde geliştirme	0	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Güvenlik	0 direnç	0	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	Sybil saldırısına direnç	0	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	Kuantum bilişime direnç	0	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Kullanım amacı	Akıllı sözleşme desteği	1	M	0	1	1	1	1	1	0	1	1	1	1	1	1	1
	Token kullanımı	0	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Üçlü çelişki	Ölçeklenebilirlik	0	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	Güvenlik	1	M														
	Merkezsizlik	0	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	Blokzincir üçlü çelişkisi (ölçeklenebilirlik, güvenlik, merkezsizlik)			0	0	1	1	1	1	1	1	1	1	1	1	1	1

Buna göre;

- Seçilen platformlar (alternatifler): Hyperledger, Quorum, Corda, OpenChain, BigchainDB, IOTA, HydraChain, Avalanche, Parity, Kadena
- Elenen Platformlar: Bitcoin, Ethereum, Stellar, Multichain biçimindedir.

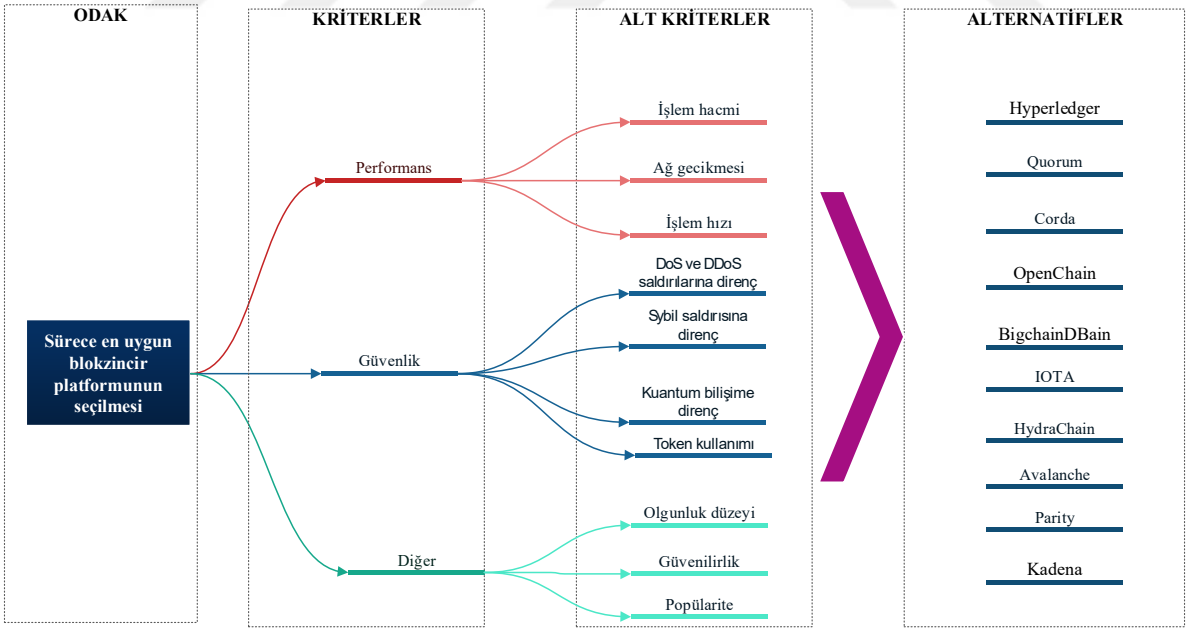
Kullanıcı girişlerine göre hazırlanmış olan, ikili karşılaştırmalar için kriter listeleri (Bkz. Çizelge 5.6'da verilmiş olan seçim kriterleri) ile Çizelge 5.9'a göre belirlenmiş olan alternatiflerin değerlendirilmesi için gerekli işlemler Analitik Hiyerarşi Prosesi ile gerçekleştirilmektedir. Bölüm 2.7.3'te detayları verilmiş olan işlem adımlarına göre, uygulaması gerçekleştirilen süreç için AHP işlemleri aşağıdaki biçimdedir:

Adım 1. Üzerinde karar verilecek durumun ve amacın tanımlanması

Uygulama konusu olarak seçilen kamu ihale sürecine en uygun blokzincir platformunun seçilmesi amaç olarak belirlenmiştir.

Adım 2. Hiyerarşik yapının oluşturulması

Daha önceki işlemler sonucunda elde edilenlere göre, hiyerarşik yapı üç kriter, 10 alt kriter ve 10 alternatiften oluşmaktadır. Verilecek karara konu temel hedef, karar verilecek konuya ilişkin kriter ve alt kriterler ile karar alternatifleri arasındaki ilişki Şekil 5.2'de verilmiştir.



Şekil 5.2. AHP hiyerarşik yapı (ihale süreci, blokzincir çözümü)

İkinci adımı takip eden 3, 4, 5 ve 6 adımlar sırasıyla ikili karşılaştırma matrislerinin oluşturulması, matrislerin normalize edilmesi, öncelik matrisinin hesaplanması ve tutarlılık analizidir. Bu adımdaki işlemlerin tamamı oluşturulan tüm matrisler için

gerçekleştirilmektedir. Oluşturulacak karşılaştırma matrisi sayısı ise kriter ve alternatif sayısına göre değişmektedir. Kamu ihale süreci uygulaması için belirlenmiş olan 10 kriter ve 10 alternatif için bu sayı 11'dir. Matrislerden ilki seçim kriterleri için ikili karşılaştırma matrisidir. Daha sonra, her bir alternatifin ayrı ayrı her bir kritere göre (10 adet) birbirleriyle karşılaştırıldığı 10 matris daha hazırlanmaktadır. Adımların daha rahat takip edilmesi ve daha kolay anlaşılması için, bir matris oluşturulduktan sonra 3 – 6. adımlardaki işlemler tamamlanmakta, daha sonra takip eden matris oluşturularak aynı işlemler gerçekleştirilmektedir.

Adım 3. İkili karşılaştırma matrislerinin oluşturulması:

Birbirlerine göre önem derecelerini belirten ifadelere göre seçim kriterleri için ikili karşılaştırma matrisleri hazırlanmaktadır. Buna göre, seçim kriterleri ikili karşılaştırma matrisi Çizelge 5.10'da (Çizelge 5.6'daki kesirli ifadeler ondalıklı değerlere dönüştürülerek) verilmiştir

Çizelge 5.10. Seçim kriterleri ikili karşılaştırma matrisi

Kriterler (ikili karşılaştırma matrisi)	Güvenilirlik	Olgunluk	Popülarite	Sybil direnci	Kuantum direnci	DoS& DDoS direnci	Ağ gecikmesi	İşlem hacmi	İşlem hızı	Token kullanımı
Güvenilirlik	1	3	4	5	6	7	8	8	8	9
Olgunluk	0,333	1	2	3	4	5	6	6	6	8
Popülarite	0,250	0,500	1	2	3	4	5	5	5	7
Sybil direnci	0,200	0,333	0,500	1	2	3	4	4	4	6
Kuantum direnci	0,167	0,250	0,333	0,500	1	2	3	3	3	5
DoS&DDoS dir.	0,143	0,200	0,250	0,333	0,500	1	2	2	2	4
Ağ gecikmesi	0,125	0,167	0,200	0,250	0,333	0,500	1	1	1	3
İşlem hacmi	0,125	0,167	0,200	0,250	0,333	0,500	1,000	1	1	3
İşlem hızı	0,125	0,167	0,200	0,250	0,333	0,500	1,000	1,000	1	3
Token kullanımı	0,111	0,125	0,143	0,167	0,200	0,250	0,333	0,333	0,333	1
TOPLAM	**2,579**	**5,908**	**8,826**	**12,75**	**17,70**	**23,750**	**31,33**	**31,333**	**31,333**	**49,000**

Adım 4. Matrislerin normalize edilmesi

Çizelge 5.10'da verilen ikili karşılaştırma matrisindeki her bir hücre değeri ilgili sütunun toplam değerine bölünerek normalize edilmektedir. Normalize edilmiş ikili karşılaştırma matrisi Çizelge 5.11'de verilmiştir.

Çizelge 5.11. Normalize edilmiş ikili karşılaştırma matrisi (N)

Kriterler (ikili karşılaştırma matrisi)	Güvenilirlik	Olgunluk	Popülarite	Sybil direnci	Kuantum direnci	DoS& DDoS direnci	Ağ gecikmesi	İşlem hacmi	İşlem hızı	Token kullanımı	**Ağırlık**
Güvenilirlik	0,388	0,508	0,453	0,392	0,339	0,295	0,255	0,255	0,255	0,184	0,332
Olgunluk	0,129	0,169	0,227	0,235	0,226	0,211	0,191	0,191	0,191	0,163	0,193
Popülarite	0,097	0,085	0,113	0,157	0,169	0,168	0,160	0,160	0,160	0,143	0,141
Sybil direnci	0,078	0,056	0,057	0,078	0,113	0,126	0,128	0,128	0,128	0,122	0,101
Kuantum direnci	0,065	0,042	0,038	0,039	0,056	0,084	0,096	0,096	0,096	0,102	0,071
DoS& DDoS direnci	0,055	0,034	0,028	0,026	0,028	0,042	0,064	0,064	0,064	0,082	0,049
Ağ gecikmesi	0,048	0,028	0,023	0,020	0,019	0,021	0,032	0,032	0,032	0,061	0,032
İşlem hacmi	0,048	0,028	0,023	0,020	0,019	0,021	0,032	0,032	0,032	0,061	0,032
İşlem hızı	0,048	0,028	0,023	0,020	0,019	0,021	0,032	0,032	0,032	0,061	0,032
Token kullanımı	0,043	0,021	0,016	0,013	0,011	0,011	0,011	0,011	0,011	0,020	0,017
TOPLAM	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000

Adım 5. Öncelik vektörünün hesaplanması:

Çizelge 5.11'de verilmiş olan normalize edilmiş matrisin "Ağırlık" başlıklı sütunu, her bir ilgili satırdaki değerlerin ortalamasını ifade etmekte olup bu ortalama değerler öncelik vektörüdür. Buna göre, seçim kriterleri öncelik vektörü Çizelge 5.12'de verilmiştir.

Çizelge 5.12. Öncelik Vektörü – Kriterler arası (Ö)

Kriter	**Öncelik Vektörü**
Güvenilirlik	0,332
Olgunluk	0,193
Popülarite	0,141
Sybil direnci	0,101
Kuantum direnci	0,071
DoS& DDoS direnci	0,049
Ağ gecikmesi	0,032
İşlem hacmi	0,032
İşlem hızı	0,032
Token kullanımı	0,017

Adım 6. Tutarlılık analizinin yapılması

Bir matrisin tutarlı olması için her i, j ve k değeri için aij.ajk=aik eşitliği sağlanmalıdır. Verilen örnekteki matris (Bkz. Çizelge 5.10) bu şartı sağlamadığından tutarsız olarak nitelendirilmektedir. Örneğin, matrise göre (Güvenilirlik, Kuantum direnci) = 6 iken (Kuantum direnci, İşlem hacmi) = 3 olduğundan matrisin tutarlı olması için (Güvenilirlik;

İşlem hacmi) = (Güvenilirlik, Kuantum direnci) x (Kuantum direnci, İşlem hacmi) eşitliği sağlanmalıdır. Ancak, matriste (Güvenilirlik; İşlem hacmi) değeri 8, eşitliğin sağ tarafındaki çarpım değeri ise (6 x 3) = 18'dir. Matristeki (Güvenilirlik; İşlem hacmi) karşılaştırmasına denk gelen (1, 8) pozisyonunun değeri olan 8, tutarlılık için gerekli olan 18 değerinden küçüktür. Bu değerin karşılık değeri ise (8, 1) pozisyonundaki 1/8 olup bu değer de tutarlılık için gerekli olan 18'nin karşılığı olan 1/18'den büyüktür. Yani, bir değer ilgili tutarlılık değerini aşarken bunun karşılığı olan değer ise tutarlılık değerinin altında kalmaktadır. Bunun anlamı, matris içerisinde tutarsızlığı telafi etme eğiliminin olmasıdır. 'n' boyutlu pozitif karşılıklı (reciprocal) bir matris tutarlı olduğunda ana özdeğer (principal eigenvalue) 'n' değerini alır. Tutarsız olduğunda ise özdeğer n'i aşar ve bu aşım değeri tutarsızlığın derecesini gösterir. Tutarlılık Oranı (Consistency Ratio – CR) olarak ifade edilen bu derece kullanılarak karşılaştırma matrisinin tutarlılığı hesaplanır.

İlgili tutarlılık analizi formülleri (Bkz. Eş. 2.6, 2.7 ve 2.8) kullanılarak yapılan hesaplama sonucunda elde edilen değerleri içeren, normalize edilmiş matris ile öncelik vektörünün çarpımı ile elde edilmiş olan matris Çizelge 5.13'te verilmiştir.

Çizelge 5.13. Seçim kriterleri (platform özellikleri) için tutarlılık analizi değerleri (NxÖ)

Kriterler (ikili karşılaştırma matrisi)	Güvenilirlik	Olgunluk	Popülarite	Sybil direnci	Kuantum direnci	DoS& DDoS direnci	Ağ gecikmesi	İşlem hacmi	İşlem hızı	Token kullanımı	**Toplam**	**Ağırlık (Önc. Vektörü)**	**Toplam/ Ağırlık**
Güvenilirlik	0,332	0,580	0,564	0,507	0,428	0,341	0,253	0,253	0,253	0,151	3,662	0,332	11,017
Olgunluk	0,111	0,193	0,282	0,304	0,286	0,244	0,189	0,189	0,189	0,134	2,122	0,193	10,970
Popülarite	0,083	0,097	0,141	0,203	0,214	0,195	0,158	0,158	0,158	0,117	1,524	0,141	10,798
Sybil direnci	0,066	0,064	0,071	0,101	0,143	0,146	0,126	0,126	0,126	0,101	1,071	0,101	10,568
Kuantum direnci	0,055	0,048	0,047	0,051	0,071	0,097	0,095	0,095	0,095	0,084	0,738	0,071	10,343
DoS& DDoS dir.	0,047	0,039	0,035	0,034	0,036	0,049	0,063	0,063	0,063	0,067	0,496	0,049	10,185
Ağ gecikmesi	0,042	0,032	0,028	0,025	0,024	0,024	0,032	0,032	0,032	0,050	0,321	0,032	10,151
İşlem hacmi	0,042	0,032	0,028	0,025	0,024	0,024	0,032	0,032	0,032	0,050	0,321	0,032	10,151
İşlem hızı	0,042	0,032	0,028	0,025	0,024	0,024	0,032	0,032	0,032	0,050	0,321	0,032	10,151
Token kullanımı	0,037	0,024	0,020	0,017	0,014	0,012	0,011	0,011	0,011	0,017	0,173	0,017	10,318
TOPLAM	0,857	1,143	1,246	1,293	1,264	1,157	0,990	0,990	0,990	0,821			
Ortalama (λ_{max})													10,465
CI $[(\lambda_{max} - n)/(n-1)]$													0,051681892
RI (Çizelge 2.42'de yer alan Rassal Indeks değerlerinden n=10'a karşılık gelen)													1,485
CR=CI/RI													0,034802621
Limit													0,10 (%10)
CR < Limit olduğundan tutarlıdır.													

Çizelge 5.13'te 'Toplam/Ağırlık' sütununun ortalaması λ_{max} değerini vermektedir. Buna göre;

- $CI = \frac{\lambda_{max}-n}{n-1} = \frac{10,465-10}{9} = 0,0517$ bulunur. Daha sonra Çizelge 2.42'de yer alan Rassal İndeks değerlerinden n=10'a karşılık gelen değer bulunarak Tutarlılık Oranı (CR) hesaplanır. Kriter sayısı 10 olduğundan RI değeri 1,485'tir. Buna göre;
  $CR = \frac{CI}{RI} = \frac{0,0517}{1,485} \approx 0,0348$ bulunur. Bu değer limit değer olan 0,10'dan küçük olduğu için karşılaştırma matrisi tutarlıdır ve sonraki işlem adımlarına devam edilebilir.

Sonraki aşamada, platform alternatifleri her bir seçim kriterine göre ayrı ayrı birbirleri ile karşılaştırılmaktadır.

Platform alternatiflerinin her bir seçim kriterine göre ikili karşılaştırmaları

Bu karşılaştırmalar için kullanılacak bilgi, modelin birinci adımı olan bilgi tabanı adımında hazırlanmış olan ve Çizelge 4.7'de verilmiş olan platform karşılaştırma tablosundan alınmaktadır. Hatırlanacağı üzere, belirlenmiş olan 14 platform alternatifi önceki adımlarda değerlendirilmiş, bunlardan dördü (Bitcoin, Ethereum, Stellar, Multichain) süreç özellikleri ve tercihler doğrultusunda elenmiştir. Buna göre kalan 10 platformun değerlendirme kriterlerine göre özellikleri Çizelge 5.14'te verilmiştir.

Çizelge 5.14. Blokzincir platformlarının seçim kriterlerine göre özellikleri

Özellik	**Hyperledger**	**Quorum**	**Corda**	**OpenChain**	**BigchainDB**	**IOTA**	**HydraChain**	**Avalanche**	**Parity**	**Kadena**
Güvenilirlik -1	5	4	4	2	3	3	2	3	3	2
Olgunluk - 2	5	4	4	3	4	3	2	3	2	3
Pazardaki popülarite - 3	5	4	4	3	3	4	3	4	4	2
Sybil saldırısına direnç - 4	3	3	3	3	3	3	3	3	3	3
Kuantum bilişim riskine direnç - 5	1	1	3	3	3	3	3	3	3	3
DoS ve DDoS saldırılarına direnç - 6	3	1	3	3	3	3	3	3	3	3
Ağ gecikmesi - 7	2	1	1	1	1	2	1	2	3	1
İşlem hacmi (saniyede işlem sayısı) - 8	3	2	5	5	2	4	2	3	5	4
İşlem hızı - 9	3	5	5	5	4	3	3	3	3	2
Token kullanımı - 10	2	1	1	1	1	1	1	1	1	1

Çizelge 5.14'te verilmiş olan değerlerin karşılıkları aşağıdaki biçimdedir:

- Güvenilirlik, Olgunluk, Pazardaki popülarite, Ağ gecikmesi, İşlem hacmi (saniyede işlem sayısı), İşlem hızı için: Çok düşük (1), Düşük (2), Orta (3), Yüksek (4) Çok yüksek (5)
- Sybil saldırısına direnç, Kuantum bilişim riskine direnç, DoS ve DDoS saldırılarına direnç için: Düşük (1), Orta (2), Yüksek (3)
- Token kullanımı için: Evet (1), Hayır (2)

Bu tabloda yer verilmiş olan özelliklere göre her bir seçim kriteri için platform özellikleri açıklanmakta, bu açıklamalara göre matrisler oluşturularak hesaplamalar yapılmaktadır. 10 kriter için yapılmış olan bu hesaplamalar ayrı başlıklar halinde aşağıda verilmiştir.

Güvenilirlik

Özellik	**Hyperledger**	**Quorum**	**Corda**	**OpenChain**	**BigchainDB**	**IOTA**	**HydraChain**	**Avalanche**	**Parity**	**Kadena**
Güvenilirlik -1	5	4	4	2	3	3	2	3	3	2

Platform alternatiflerinin "güvenilirlik" kriterine göre özellikleri aşağıdaki biçimdedir:

- Hyperledger platformu güvenilirliği "Çok yüksek" olan tek platformdur.
- Quorum ve Corda platformları güvenilirliği "Yüksek" olan platformlardır. Birbirlerine göre önem dereceleri eşittir.
- BigchainDB, IOTA, Avalanche ve Parity platformları güvenilirliği "Orta" olan platformlardır. Birbirlerine göre önem dereceleri eşittir.
- OpenChain, HydraChain ve Kadena platformları güvenilirliği "Düşük" olan platformlardır. Birbirlerine göre önem dereceleri eşittir.
- 1 – 5 skalasında değerlendirilmiş olan güvenilirlik özelliği için Hyperledger;
  - Quorum ve Corda'ya göre biraz daha önemli (3),
  - BigchainDB, IOTA, Avalanche ve Parity'ye göre esaslı veya güçlü önemde (5),
  - OpenChain, HydraChain ve Kadena'ya göre ise çok güçlü önemdedir (7).
- 1 – 5 skalasında değerlendirilmiş olan güvenilirlik özelliği için eşit önemde olan Quorum ve Corda;
  - BigchainDB, IOTA, Avalanche ve Parity'ye göre biraz daha önemli (3),

  - OpenChain, HydraChain ve Kadena'ya göre esaslı veya güçlü önemdedir (5).
- 1 – 5 skalasında değerlendirilmiş olan güvenilirlik özelliği için eşit önemde olan BigchainDB, IOTA, Avalanche ve Parity:
  - OpenChain, HydraChain ve Kadena'ya göre biraz daha önemlidir (3).
- OpenChain, HydraChain ve Kadena birbiri ile eşit önemdedir.

Verilen bu bilgilere göre güvenilirlik kriterine göre alternatiflerin birbirlerine göre önem derecelerini gösteren ikili karşılaştırma matrisi Çizelge 5.15'te verilmiştir.

Çizelge 5.15. Güvenilirlik kriterine göre alternatiflerin ikili karşılaştırma matrisi

GÜVENİLİRLİK	Hyperledger	Quorum	Corda	OpenChain	BigchainDB	IOTA	HydraChain	Avalanche	Parity	Kadena
Hyperledger	1	3	3	7	5	5	7	5	5	7
Quorum	0,333	1	1	5	3	3	5	3	3	5
Corda	0,333	1,000	1	5	3	3	5	3	3	5
OpenChain	0,143	0,200	0,200	1	0,333	0,333	1	0,333	0,333	1
BigchainDB	0,200	0,333	0,333	3,000	1	1	3	1	1	3
IOTA	0,200	0,333	0,333	3,000	1,000	1	3	1	1	3
HydraChain	0,143	0,200	0,200	1,000	0,333	0,333	1	0,333	0,333	1
Avalanche	0,200	0,333	0,333	3,000	1,000	1,000	3,000	1	1	3
Parity	0,200	0,333	0,333	3,000	1,000	1,000	3,000	1,000	1	3
Kadena	0,143	0,200	0,200	1,000	0,333	0,333	1,000	0,333	0,333	1
TOPLAM	2,895	6,933	6,933	32,000	16,000	16,000	32,000	16,000	16,000	32,000

Adım 4. Matrislerin normalize edilmesi: Çizelge 5.15'te verilen ikili karşılaştırma matrisindeki her bir hücre değeri ilgili sütunun toplam değerine bölünerek normalize edilmektedir. Normalize edilmiş ikili karşılaştırma matrisi Çizelge 5.16'da verilmiştir.

Çizelge 5.16. Normalize edilmiş ikili karşılaştırma matrisi - Güvenilirlik (N)

GÜVENİLİRLİK	Hyperledger	Quorum	Corda	OpenChain	BigchainDB	IOTA	HydraChain	Avalanche	Parity	Kadena	Ağırlık
Hyperledger	0,345	0,433	0,433	0,219	0,313	0,313	0,219	0,313	0,313	0,219	0,312
Quorum	0,115	0,144	0,144	0,156	0,188	0,188	0,156	0,188	0,188	0,156	0,162
Corda	0,115	0,144	0,144	0,156	0,188	0,188	0,156	0,188	0,188	0,156	0,162
OpenChain	0,049	0,029	0,029	0,031	0,021	0,021	0,031	0,021	0,021	0,031	0,028
BigchainDB	0,069	0,048	0,048	0,094	0,063	0,063	0,094	0,063	0,063	0,094	0,070

GÜVENİLİRLİK	Hyperledger	Quorum	Corda	OpenChain	BigchainDB	IOTA	HydraChain	Avalanche	Parity	Kadena	Ağırlık
IOTA	0,069	0,048	0,048	0,094	0,063	0,063	0,094	0,063	0,063	0,094	0,070
HydraChain	0,049	0,029	0,029	0,031	0,021	0,021	0,031	0,021	0,021	0,031	0,028
Avalanche	0,069	0,048	0,048	0,094	0,063	0,063	0,094	0,063	0,063	0,094	0,070
Parity	0,069	0,048	0,048	0,094	0,063	0,063	0,094	0,063	0,063	0,094	0,070
Kadena	0,049	0,029	0,029	0,031	0,021	0,021	0,031	0,021	0,021	0,031	0,028
TOPLAM	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000

Adım 5. Öncelik vektörünün hesaplanması: Çizelge 5.16'da verilmiş olan normalize edilmiş matrisin "Ağırlık" başlıklı sütunu, her bir ilgili satırdaki değerlerin ortalamasını ifade etmekte olup bu ortalama değerler öncelik vektörüdür. Buna göre, seçim kriterleri öncelik vektörü Çizelge 5.17'de verilmiştir.

Çizelge 5.17. Öncelik Vektörü – Güvenilirlik (Ö)

Alternatif	Öncelik Vektörü
Hyperledger	0,312
Quorum	0,162
Corda	0,162
OpenChain	0,028
BigchainDB	0,070
IOTA	0,070
HydraChain	0,028
Avalanche	0,070
Parity	0,070
Kadena	0,028

Adım 6. Tutarlılık analizinin yapılması: İlgili tutarlılık analizi formülleri (Bkz. Eş. 2.6, 2.7 ve 2.8) kullanılarak yapılan hesaplama sonucunda elde edilen değerleri içeren, normalize edilmiş matris ile öncelik vektörünün çarpımı ile elde edilmiş olan matris Çizelge 5.18'de verilmiştir.

Çizelge 5.18. Tutarlılık analizi tablosu - Güvenilirlik (NxÖ)

GÜVENİLİRLİK	Hyperledger	Quorum	Corda	OpenChain	BigchainDB	IOTA	HydraChain	Avalanche	Parity	Kadena	Toplam	Ağırlık	Ağırlık (Önc. Vektörü)
Hyperledger	0,312	0,487	0,487	0,199	0,348	0,348	0,199	0,348	0,348	0,199	3,275	0,312	10,506

GÜVENİLİRLİK	Hyperledger	Quorum	Corda	OpenChain	BigchainDB	IOTA	HydraChain	Avalanche	Parity	Kadena	Toplam	Ağırlık	Ağırlık (Önc. Vektörü)
Quorum	0,104	0,162	0,162	0,142	0,209	0,209	0,142	0,209	0,209	0,142	1,690	0,162	10,419
Corda	0,104	0,162	0,162	0,142	0,209	0,209	0,142	0,209	0,209	0,142	1,690	0,162	10,419
OpenChain	0,045	0,032	0,032	0,028	0,023	0,023	0,028	0,023	0,023	0,028	0,288	0,028	10,120
BigchainDB	0,062	0,054	0,054	0,085	0,070	0,070	0,085	0,070	0,070	0,085	0,705	0,070	10,119
IOTA	0,062	0,054	0,054	0,085	0,070	0,070	0,085	0,070	0,070	0,085	0,705	0,070	10,119
HydraChain	0,045	0,032	0,032	0,028	0,023	0,023	0,028	0,023	0,023	0,028	0,288	0,028	10,120
Avalanche	0,062	0,054	0,054	0,085	0,070	0,070	0,085	0,070	0,070	0,085	0,705	0,070	10,119
Parity	0,062	0,054	0,054	0,085	0,070	0,070	0,085	0,070	0,070	0,085	0,705	0,070	10,119
Kadena	0,045	0,032	0,032	0,028	0,023	0,023	0,028	0,023	0,023	0,028	0,288	0,028	10,120
TOPLAM	0,902	1,125	1,125	0,909	1,114	1,114	0,909	1,114	1,114	0,909			
Ortalama (λ_{max})													10,218
CI $[(\lambda_{max} - n)/(n-1)]$													0,024232384
RI (Çizelge 2.42'de yer alan Rassal Indeks değerlerinden n=10'a karşılık gelen)													1,485
CR=CI/RI													0,016318103
Limit													0,10 (%10)
CR < Limit olduğundan tutarlıdır.													

CR değeri limit değer olan 0,10'dan küçük olduğu için karşılaştırma matrisi tutarlıdır ve sonraki işlem adımlarına devam edilebilir.

Olgunluk

Özellik	**Hyperledger**	**Quorum**	**Corda**	**OpenChain**	**BigchainDB**	**IOTA**	**HydraChain**	**Avalanche**	**Parity**	**Kadena**
Olgunluk - 2	5	4	4	3	4	3	2	3	2	3

Platform alternatiflerinin "olgunluk" kriterine göre özellikleri aşağıdaki biçimdedir:

- Hyperledger platformu olgunluğu "Çok yüksek" olan tek platformdur.
- Quorum, Corda ve BigchainDB platformları güvenilirliği "Yüksek" olan platformlardır. Birbirlerine göre önem dereceleri eşittir.
- OpenChain, IOTA, Avalanche ve Kadena olgunluğu "Orta" olan platformlardır. Birbirlerine göre önem dereceleri eşittir.
- HydraChain ve Parity olgunluğu "Düşük" olan platformlardır. Birbirlerine göre önem dereceleri eşittir.

- 1 – 5 skalasında değerlendirilmiş olan olgunluk özelliği için Hyperledger;
  - Quorum, Corda ve BigchainDB'ye göre biraz daha önemli (3),
  - OpenChain, IOTA, Avalanche ve Kadena'ya göre esaslı veya güçlü önemde (5),
  - HydraChain ve Parity'ye göre ise çok güçlü önemdedir (7).
- 1 – 5 skalasında değerlendirilmiş olan olgunluk özelliği için eşit önemde olan Quorum, Corda ve BigchainDB;
  - OpenChain, IOTA, Avalanche ve Kadena'ya göre biraz daha önemli (3),
  - HydraChain ve Parity'ye göre ise esaslı veya güçlü önemdedir (5).
- 1 – 5 skalasında değerlendirilmiş olan olgunluk özelliği için eşit önemde olan OpenChain, IOTA, Avalanche ve Kadena;
  - HydraChain ve Parity'ye göre biraz daha önemlidir (3).
- HydraChain ve Parity birbiri ile eşit önemdedir.

Verilen bu bilgilere göre olgunluk kriterine göre alternatiflerin birbirlerine göre önem derecelerini gösteren ikili karşılaştırma matrisi Çizelge 5.19'da verilmiştir.

Çizelge 5.19. Olgunluk kriterine göre alternatiflerin ikili karşılaştırma matrisi

OLGUNLUK	Hyperledger	Quorum	Corda	OpenChain	BigchainDB	IOTA	HydraChain	Avalanche	Parity	Kadena
Hyperledger	1	3,000	3,000	5,000	3,000	5,000	7,000	5,000	7,000	5,000
Quorum	0,333	1	1,000	3,000	1,000	3,000	5,000	3,000	5,000	3,000
Corda	0,333	1,000	1	3,000	1,000	3,000	5,000	3,000	5,000	3,000
OpenChain	0,200	0,333	0,333	1	0,333	1,000	3,000	1,000	3,000	1,000
BigchainDB	0,333	1,000	1,000	3,000	1	3,000	5,000	3,000	5,000	3,000
IOTA	0,200	0,333	0,333	1,000	0,333	1	3,000	1,000	3,000	1,000
HydraChain	0,143	0,200	0,200	0,333	0,200	0,333	1	0,333	1,000	0,333
Avalanche	0,200	0,333	0,333	1,000	0,333	1,000	3,000	1	3,000	1,000
Parity	0,143	0,200	0,200	0,333	0,200	0,333	1,000	0,333	1	0,333
Kadena	0,200	0,333	0,333	1,000	0,333	1,000	3,000	1,000	3,000	1
TOPLAM	3,086	7,733	7,733	18,667	7,733	18,667	36,000	18,667	36,000	18,667

Adım 4. Matrislerin normalize edilmesi: Çizelge 5.19'da verilen ikili karşılaştırma matrisindeki her bir hücre değeri ilgili sütunun toplam değerine bölünerek normalize edilmektedir. Normalize edilmiş ikili karşılaştırma matrisi Çizelge 5.20'de verilmiştir.

Çizelge 5.20. Normalize edilmiş ikili karşılaştırma matrisi - Olgunluk (N)

OLGUNLUK	Hyperledger	Quorum	Corda	OpenChain	BigchainDB	IOTA	HydraChain	Avalanche	Parity	Kadena	Ağırlık
Hyperledger	0,324	0,388	0,388	0,268	0,388	0,268	0,194	0,268	0,194	0,268	0,295
Quorum	0,108	0,129	0,129	0,161	0,129	0,161	0,139	0,161	0,139	0,161	0,142
Corda	0,108	0,129	0,129	0,161	0,129	0,161	0,139	0,161	0,139	0,161	0,142
OpenChain	0,065	0,043	0,043	0,054	0,043	0,054	0,083	0,054	0,083	0,054	0,058
BigchainDB	0,108	0,129	0,129	0,161	0,129	0,161	0,139	0,161	0,139	0,161	0,142
IOTA	0,065	0,043	0,043	0,054	0,043	0,054	0,083	0,054	0,083	0,054	0,058
HydraChain	0,046	0,026	0,026	0,018	0,026	0,018	0,028	0,018	0,028	0,018	0,025
Avalanche	0,065	0,043	0,043	0,054	0,043	0,054	0,083	0,054	0,083	0,054	0,058
Parity	0,046	0,026	0,026	0,018	0,026	0,018	0,028	0,018	0,028	0,018	0,025
Kadena	0,065	0,043	0,043	0,054	0,043	0,054	0,083	0,054	0,083	0,054	0,058
TOPLAM	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000

Adım 5. Öncelik vektörünün hesaplanması: Çizelge 5.20'de verilmiş olan normalize edilmiş matrisin "Ağırlık" başlıklı sütunu, her bir ilgili satırdaki değerlerin ortalamasını ifade etmekte olup bu ortalama değerler öncelik vektörüdür. Buna göre, seçim kriterleri öncelik vektörü Çizelge 5.21'de verilmiştir.

Çizelge 5.21. Öncelik Vektörü – Olgunluk (Ö)

Alternatif	**Öncelik Vektörü**
Hyperledger	0,295
Quorum	0,142
Corda	0,142
OpenChain	0,058
BigchainDB	0,142
IOTA	0,058
HydraChain	0,025
Avalanche	0,058
Parity	0,025
Kadena	0,058

Adım 6. Tutarlılık analizinin yapılması: İlgili tutarlılık analizi formülleri (Bkz. Eş. 2.6, 2.7 ve 2.8) kullanılarak yapılan hesaplama sonucunda elde edilen değerleri içeren, normalize edilmiş matris ile öncelik vektörünün çarpımı ile elde edilmiş olan matris Çizelge 5.22'de verilmiştir.

Çizelge 5.22. Tutarlılık analizi tablosu - Olgunluk (NxÖ)

OLGUNLUK	Hyperledger	Quorum	Corda	OpenChain	BigchainDB	IOTA	HydraChain	Avalanche	Parity	Kadena	Toplam	Ağırlık	Ağırlık (Önc. Vektörü)
Hyperledger	0,295	0,425	0,425	0,288	0,425	0,288	0,176	0,288	0,176	0,288	3,071	0,295	10,417
Quorum	0,098	0,142	0,142	0,173	0,142	0,173	0,125	0,173	0,125	0,173	1,464	0,142	10,336
Corda	0,098	0,142	0,142	0,173	0,142	0,173	0,125	0,173	0,125	0,173	1,464	0,142	10,336
OpenChain	0,059	0,047	0,047	0,058	0,047	0,058	0,075	0,058	0,075	0,058	0,581	0,058	10,106
BigchainDB	0,098	0,142	0,142	0,173	0,142	0,173	0,125	0,173	0,125	0,173	1,464	0,142	10,336
IOTA	0,059	0,047	0,047	0,058	0,047	0,058	0,075	0,058	0,075	0,058	0,581	0,058	10,106
HydraChain	0,042	0,028	0,028	0,019	0,028	0,019	0,025	0,019	0,025	0,019	0,254	0,025	10,123
Avalanche	0,059	0,047	0,047	0,058	0,047	0,058	0,075	0,058	0,075	0,058	0,581	0,058	10,106
Parity	0,042	0,028	0,028	0,019	0,028	0,019	0,025	0,019	0,025	0,019	0,254	0,025	10,123
Kadena	0,059	0,047	0,047	0,058	0,047	0,058	0,075	0,058	0,075	0,058	0,581	0,058	10,106
TOPLAM	0,910	1,095	1,095	1,073	1,095	1,073	0,903	1,073	0,903	1,073			
Ortalama (λ_{max})													10,210
CI $[(\lambda_{max} - n)/(n-1)]$													0,023292169
RI (Çizelge 2.42'de yer alan Rassal Indeks değerlerinden n=10'a karşılık gelen)													1,485
CR=CI/RI													0,015684962
Limit													0,10 (%10)
CR < Limit olduğundan tutarlıdır.													

CR değeri limit değer olan 0,10'dan küçük olduğu için karşılaştırma matrisi tutarlıdır ve sonraki işlem adımlarına devam edilebilir.

Popülarite

Özellik	**Hyperledger**	**Quorum**	**Corda**	**OpenChain**	**BigchainDB**	**IOTA**	**HydraChain**	**Avalanche**	**Parity**	**Kadena**
Pazardaki popülarite - 3	5	4	4	3	3	4	3	4	4	2

Platform alternatiflerinin "popülarite" kriterine göre özellikleri aşağıdaki biçimdedir:

- Hyperledger platformu popülerliği "Çok yüksek" olan tek platformdur.
- Quorum, Corda, IOTA, Avalanche ve Parity platformları popülerliği "Yüksek" olan platformlardır. Birbirlerine göre önem dereceleri eşittir.
- OpenChain, BigchainDB ve HydraChain platformları popülerliği "Orta" olan platformlardır. Birbirlerine göre önem dereceleri eşittir.

- Kadena platformu popülerliği “Düşük” olan tek platformdur.
- 1 – 5 skalasında değerlendirilmiş olan popülerlik özelliği için Hyperledger;
  - Quorum, Corda, IOTA, Avalanche ve Parity’ye göre biraz daha önemli (3),
  - OpenChain, BigchainDB ve HydraChain’e göre esaslı veya güçlü önemde (5),
  - Kadena’ya göre ise çok güçlü önemdedir (7).
- 1 – 5 skalasında değerlendirilmiş olan popülerlik özelliği için eşit önemde olan Quorum, Corda, IOTA, Avalanche ve Parity;
  - OpenChain, BigchainDB ve HydraChain’e göre biraz daha önemli (3),
  - Kadena’ya göre ise esaslı veya güçlü önemdedir (5).
- 1 – 5 skalasında değerlendirilmiş olan popülerlik özelliği için eşit önemde olan OpenChain, BigchainDB ve HydraChain;
  - Kadena’ya göre biraz daha önemlidir (3).

Verilen bu bilgilere göre popülarite kriterine göre alternatiflerin birbirlerine göre önem derecelerini gösteren ikili karşılaştırma matrisi Çizelge 5.23’te verilmiştir.

Çizelge 5.23. Popülarite kriterine göre alternatiflerin ikili karşılaştırma matrisi

POPÜLARİTE	Hyperledger	Quorum	Corda	OpenChain	BigchainDB	IOTA	HydraChain	Avalanche	Parity	Kadena
Hyperledger	1	3,000	3,000	5,000	5,000	3,000	5,000	3,000	3,000	7,000
Quorum	0,333	1	1,000	3,000	3,000	1,000	3,000	1,000	1,000	5,000
Corda	0,333	1,000	1	3,000	3,000	1,000	3,000	1,000	1,000	5,000
OpenChain	0,200	0,333	0,333	1	1,000	0,333	1,000	0,333	0,333	3,000
BigchainDB	0,200	0,333	0,333	1,000	1	0,333	1,000	0,333	0,333	3,000
IOTA	0,333	1,000	1,000	3,000	3,000	1	3,000	1,000	1,000	5,000
HydraChain	0,200	0,333	0,333	1,000	1,000	0,333	1	0,333	0,333	3,000
Avalanche	0,333	1,000	1,000	3,000	3,000	1,000	3,000	1	1,000	5,000
Parity	0,333	1,000	1,000	3,000	3,000	1,000	3,000	1,000	1	5,000
Kadena	0,143	0,200	0,200	0,333	0,333	0,200	0,333	0,200	0,200	1
TOPLAM	3,410	9,200	9,200	23,333	23,333	9,200	23,333	9,200	9,200	42,000

Adım 4. Matrislerin normalize edilmesi: Çizelge 5.23’te verilen ikili karşılaştırma matrisindeki her bir hücre değeri ilgili sütunun toplam değerine bölünerek normalize edilmektedir. Normalize edilmiş ikili karşılaştırma matrisi Çizelge 5.24’te verilmiştir.

Çizelge 5.24. Normalize edilmiş ikili karşılaştırma matrisi - Popülarite (N)

POPÜLARİTE	Hyperledger	Quorum	Corda	OpenChain	BigchainDB	IOTA	HydraChain	Avalanche	Parity	Kadena	Ağırlık
Hyperledger	0,293	0,326	0,326	0,214	0,214	0,326	0,214	0,326	0,326	0,167	0,273
Quorum	0,098	0,109	0,109	0,129	0,129	0,109	0,129	0,109	0,109	0,119	0,115
Corda	0,098	0,109	0,109	0,129	0,129	0,109	0,129	0,109	0,109	0,119	0,115
OpenChain	0,059	0,036	0,036	0,043	0,043	0,036	0,043	0,036	0,036	0,071	0,044
BigchainDB	0,059	0,036	0,036	0,043	0,043	0,036	0,043	0,036	0,036	0,071	0,044
IOTA	0,098	0,109	0,109	0,129	0,129	0,109	0,129	0,109	0,109	0,119	0,115
HydraChain	0,059	0,036	0,036	0,043	0,043	0,036	0,043	0,036	0,036	0,071	0,044
Avalanche	0,098	0,109	0,109	0,129	0,129	0,109	0,129	0,109	0,109	0,119	0,115
Parity	0,098	0,109	0,109	0,129	0,129	0,109	0,129	0,109	0,109	0,119	0,115
Kadena	0,042	0,022	0,022	0,014	0,014	0,022	0,014	0,022	0,022	0,024	0,022
TOPLAM	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000

Adım 5. Öncelik vektörünün hesaplanması: Çizelge 5.24'te verilmiş olan normalize edilmiş matrisin "Ağırlık" başlıklı sütunu, her bir ilgili satırdaki değerlerin ortalamasını ifade etmekte olup bu ortalama değerler öncelik vektörüdür. Buna göre, seçim kriterleri öncelik vektörü Çizelge 5.25'te verilmiştir.

Çizelge 5.25. Öncelik Vektörü – Popülarite (Ö)

Alternatif	Öncelik Vektörü
Hyperledger	0,273
Quorum	0,115
Corda	0,115
OpenChain	0,044
BigchainDB	0,044
IOTA	0,115
HydraChain	0,044
Avalanche	0,115
Parity	0,115
Kadena	0,022

Adım 6. Tutarlılık analizinin yapılması: İlgili tutarlılık analizi formülleri (Bkz. Eş. 2.6, 2.7 ve 2.8) kullanılarak yapılan hesaplama sonucunda elde edilen değerleri içeren, normalize edilmiş matris ile öncelik vektörünün çarpımı ile elde edilmiş olan matris Çizelge 5.26'da verilmiştir.

Çizelge 5.26. Tutarlılık analizi tablosu – Popülarite (NxÖ)

POPÜLARİTE	**Hyperledger**	**Quorum**	**Corda**	**OpenChain**	**BigchainDB**	**IOTA**	**HydraChain**	**Avalanche**	**Parity**	**Kadena**	**Toplam**	**Ağırlık**	**Ağırlık (Önc. Vektörü)**
Hyperledger	0,273	0,344	0,344	0,220	0,220	0,344	0,220	0,344	0,344	0,152	2,804	0,273	10,259
Quorum	0,091	0,115	0,115	0,132	0,132	0,115	0,132	0,115	0,115	0,109	1,169	0,115	10,197
Corda	0,091	0,115	0,115	0,132	0,132	0,115	0,132	0,115	0,115	0,109	1,169	0,115	10,197
OpenChain	0,055	0,038	0,038	0,044	0,044	0,038	0,044	0,038	0,038	0,065	0,443	0,044	10,068
BigchainDB	0,055	0,038	0,038	0,044	0,044	0,038	0,044	0,038	0,038	0,065	0,443	0,044	10,068
IOTA	0,091	0,115	0,115	0,132	0,132	0,115	0,132	0,115	0,115	0,109	1,169	0,115	10,197
HydraChain	0,055	0,038	0,038	0,044	0,044	0,038	0,044	0,038	0,038	0,065	0,443	0,044	10,068
Avalanche	0,091	0,115	0,115	0,132	0,132	0,115	0,132	0,115	0,115	0,109	1,169	0,115	10,197
Parity	0,091	0,115	0,115	0,132	0,132	0,115	0,132	0,115	0,115	0,109	1,169	0,115	10,197
Kadena	0,039	0,023	0,023	0,015	0,015	0,023	0,015	0,023	0,023	0,022	0,219	0,022	10,096
TOPLAM	0,932	1,054	1,054	1,026	1,026	1,054	1,026	1,054	1,054	0,912			
Ortalama (λ_{max})													10,154
CI $[(\lambda_{max} - n)/(n-1)]$													0,017147449
RI (Çizelge 2.42'de yer alan Rassal Indeks değerlerinden n=10'a karşılık gelen)													1,485
CR=CI/RI													0,011547103
Limit													0,10 (%10)
CR < Limit olduğundan tutarlıdır.													

CR değeri limit değer olan 0,10'dan küçük olduğu için karşılaştırma matrisi tutarlıdır ve sonraki işlem adımlarına devam edilebilir.

Sybil direnci

Özellik	**Hyperledger**	**Quorum**	**Corda**	**OpenChain**	**BigchainDB**	**IOTA**	**HydraChain**	**Avalanche**	**Parity**	**Kadena**
Sybil saldırısına direnç - 4	3	3	3	3	3	3	3	3	3	3

Platform alternatiflerinin "sybil saldırısına direnç" kriterine göre özellikleri aşağıdaki biçimdedir:

- Sybil saldırısına direnç bakımından tüm platformlar eşit önem derecesindedir. Platformların tamamının direnci "Yüksek"tir.
- Tüm platformların birbirlerine göre önem dereceleri "1" olduğundan ikili karşılaştırma matrisi ve normalize edilmiş matris tüm değerleri "1" olan matrislerdir. Bu nedenle bu

matrisler ayrıca gösterilmemiştir. Bu durumda, öncelik vektörü de Çizelge 5.27'de verildiği biçimdedir:

Çizelge 5.27. Öncelik Vektörü – Sybil direnci (Ö)

Alternatif	**Öncelik Vektörü**
Hyperledger	0,100
Quorum	0,100
Corda	0,100
OpenChain	0,100
BigchainDB	0,100
IOTA	0,100
HydraChain	0,100
Avalanche	0,100
Parity	0,100
Kadena	0,100

CR değeri bu durumda "0" olacağından, tutarlılık analizine gerek bulunmamakla birlikte, tutarlılığa ilişkin hesaplanan değerler Çizelge 5.28'de verilmiştir.

Çizelge 5.28. Tutarlılık analizi tablosu - Sybil Direnci (NxÖ)

Ortalama (λ_{max})	10,000
CI $[(\lambda_{max} - n)/(n-1)]$	0
RI (Çizelge 2.42'de yer alan Rassal Indeks değerlerinden n=10'a karşılık gelen)	1,485
CR=CI/RI	0
Limit	**0,10 (%10)**
CR < Limit olduğundan tutarlıdır.	

Kuantum direnci

Özellik	**Hyperledger**	**Quorum**	**Corda**	**OpenChain**	**BigchainDB**	**IOTA**	**HydraChain**	**Avalanche**	**Parity**	**Kadena**
Kuantum bilişim riskine direnç - 5	1	1	3	3	3	3	3	3	3	3

Kuantum bilişim riskine direnç değerlendirilirken "Düşük", "Orta" ve "Yüksek" olmak üzere 1-3 arasında puanlama yapılmaktadır. Platform alternatiflerinin "kuantum bilişim riskine direnç" kriterine göre özellikleri aşağıdaki biçimdedir:

- Corda, OpenChain, BigchainDB, IOTA, HydraChain, Avalanche, Parity ve Kadena kuantum bilişim riskine karşı dirençleri "yüksek" olarak değerlendirilen platformlardır ve birbirlerine göre önem dereceleri eşittir.
- Hyperledger ve Quorum platformlarının kuantum bilişim riskine karşı dirençleri "düşük" olarak değerlendirilmekte olup bu platformların birbirlerine göre önem dereceleri eşittir.
- 1 – 3 skalasında değerlendirilmiş olan kuantum direnci özelliği için eşit önemde olan Corda, OpenChain, BigchainDB, IOTA, HydraChain, Avalanche, Parity ve Kadena;
    - Hyperledger ve Quorum'a göre son derece güçlü önemdedir (9).

Verilen bu bilgilere göre kuantum direnci kriterine göre alternatiflerin birbirlerine göre önem derecelerini gösteren ikili karşılaştırma matrisi Çizelge 5.29'da verilmiştir.

Çizelge 5.29. Kuantum direnci kriterine göre alternatiflerin ikili karşılaştırma matrisi

KUANTUM DİRENCİ	Hyperledger	Quorum	Corda	OpenChain	BigchainDB	IOTA	HydraChain	Avalanche	Parity	Kadena
Hyperledger	1	1,000	0,111	0,111	0,111	0,111	0,111	0,111	0,111	0,111
Quorum	1,000	1	0,111	0,111	0,111	0,111	0,111	0,111	0,111	0,111
Corda	9,000	9,000	1	1,000	1,000	1,000	1,000	1,000	1,000	1,000
OpenChain	9,000	9,000	1,000	1	1,000	1,000	1,000	1,000	1,000	1,000
BigchainDB	9,000	9,000	1,000	1,000	1	1,000	1,000	1,000	1,000	1,000
IOTA	9,000	9,000	1,000	1,000	1,000	1	1,000	1,000	1,000	1,000
HydraChain	9,000	9,000	1,000	1,000	1,000	1,000	1	1,000	1,000	1,000
Avalanche	9,000	9,000	1,000	1,000	1,000	1,000	1,000	1	1,000	1,000
Parity	9,000	9,000	1,000	1,000	1,000	1,000	1,000	1,000	1	1,000
Kadena	9,000	9,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1
TOPLAM	74,000	74,000	8,222	8,222	8,222	8,222	8,222	8,222	8,222	8,222

Adım 4. Matrislerin normalize edilmesi: Çizelge 5.29'da verilen ikili karşılaştırma matrisindeki her bir hücre değeri ilgili sütunun toplam değerine bölünerek normalize edilmektedir. Normalize edilmiş ikili karşılaştırma matrisi Çizelge 5.30'da verilmiştir.

Çizelge 5.30. Normalize edilmiş ikili karşılaştırma matrisi - Kuantum direnci (N)

KUANTUM DİRENCİ	Hyperledger	Quorum	Corda	OpenChain	BigchainDB	IOTA	HydraChain	Avalanche	Parity	Kadena	Ağırlık
Hyperledger	0,014	0,014	0,014	0,014	0,014	0,014	0,014	0,014	0,014	0,014	0,014
Quorum	0,014	0,014	0,014	0,014	0,014	0,014	0,014	0,014	0,014	0,014	0,014
Corda	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122
OpenChain	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122
BigchainDB	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122
IOTA	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122
HydraChain	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122
Avalanche	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122
Parity	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122
Kadena	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122
TOPLAM	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000

Adım 5. Öncelik vektörünün hesaplanması: Çizelge 5.30'da verilmiş olan normalize edilmiş matrisin "Ağırlık" başlıklı sütunu, her bir ilgili satırdaki değerlerin ortalamasını ifade etmekte olup bu ortalama değerler öncelik vektörüdür. Buna göre, seçim kriterleri öncelik vektörü Çizelge 5.31'de verilmiştir.

Çizelge 5.31. Öncelik Vektörü – Kuantum direnci (Ö)

Alternatif	Öncelik Vektörü
Hyperledger	0,014
Quorum	0,014
Corda	0,122
OpenChain	0,122
BigchainDB	0,122
IOTA	0,122
HydraChain	0,122
Avalanche	0,122
Parity	0,122
Kadena	0,122

Adım 6. Tutarlılık analizinin yapılması: İlgili tutarlılık analizi formülleri (Bkz. Eş. 2.6, 2.7 ve 2.8) kullanılarak yapılan hesaplama sonucunda elde edilen değerleri içeren, normalize edilmiş matris ile öncelik vektörünün çarpımı ile elde edilmiş olan matris Çizelge 5.32'de verilmiştir.

Çizelge 5.32. Tutarlılık analizi tablosu - Kuantum direnci (NxÖ)

KUANTUM DİRENCİ	Hyperledger	Quorum	Corda	OpenChain	BigchainDB	IOTA	HydraChain	Avalanche	Parity	Kadena	Toplam	Ağırlık	Ağırlık (Önc. Vektörü)[10]
Hyperledger	0,014	0,014	0,014	0,014	0,014	0,014	0,014	0,014	0,014	0,014	0,135	0,014	10,000
Quorum	0,014	0,014	0,014	0,014	0,014	0,014	0,014	0,014	0,014	0,014	0,135	0,014	10,000
Corda	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	1,216	0,122	10,000
OpenChain	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	1,216	0,122	10,000
BigchainDB	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	1,216	0,122	10,000
IOTA	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	1,216	0,122	10,000
HydraChain	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	1,216	0,122	10,000
Avalanche	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	1,216	0,122	10,000
Parity	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	1,216	0,122	10,000
Kadena	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	0,122	1,216	0,122	10,000
TOPLAM	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000			
Ortalama (λ_{max})												10,000	
CI $[(\lambda_{max} - n)/(n-1)]$												0	
RI (Çizelge 2.42'de yer alan Rassal Indeks değerlerinden n=10'a karşılık gelen)												1,485	
CR=CI/RI												0	
Limit												**0,10 (%10)**	
CR < Limit olduğundan tutarlıdır.													

CR değeri limit değer olan 0,10'dan küçük olduğu için karşılaştırma matrisi tutarlıdır ve sonraki işlem adımlarına devam edilebilir.

DoS & DDoS direnci

Özellik	**Hyperledger**	**Quorum**	**Corda**	**OpenChain**	**BigchainDB**	**IOTA**	**HydraChain**	**Avalanche**	**Parity**	**Kadena**
DoS&DDoS saldırılarına direnç - 6	3	1	3	3	3	3	3	3	3	3

DoS ve DDoS saldırılarına karşı direnç değerlendirilirken "Düşük", "Orta" ve "Yüksek" olmak üzere 1-3 arasında puanlama yapılmaktadır. Platform alternatiflerinin "DoS ve DDoS saldırılarına karşı direnç" kriterine göre özellikleri aşağıdaki biçimdedir:

[10] Hücre değeri gösteriminde yuvarlanmış miktarlar kullanılmış, toplam/ağırlık hesabı ise değerler yuvarlanmadan yapılmıştır.

- Hyperledger, Corda, OpenChain, BigchainDB, IOTA, HydraChain, Avalanche, Parity ve Kadena DoS ve DDoS riskine karşı dirençleri "yüksek" olarak değerlendirilen platformlardır ve birbirlerine göre önem dereceleri eşittir.
- Quorum platformunun DoS ve DDoS riskine karşı direnci "düşük" olarak değerlendirilmektedir.
- 1 – 3 skalasında değerlendirilmiş olan DoS ve DDoS direnci özelliği için eşit önemde olan Hyperledger, Corda, OpenChain, BigchainDB, IOTA, HydraChain, Avalanche, Parity ve Kadena;
    - Quorum'a göre son derece güçlü önemdedir (9).

Verilen bu bilgilere göre DoS ve DDoS direnci kriterine göre alternatiflerin birbirlerine göre önem derecelerini gösteren ikili karşılaştırma matrisi Çizelge 5.33'te verilmiştir.

Çizelge 5.33. DoS ve DDoS direnci kriterine göre alternatiflerin ikili karşılaştırma matrisi

DoS & DDoS DİRENCİ	Hyperledger	Quorum	Corda	OpenChain	BigchainDB	IOTA	HydraChain	Avalanche	Parity	Kadena
Hyperledger	1	9,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000
Quorum	0,111	1	0,111	0,111	0,111	0,111	0,111	0,111	0,111	0,111
Corda	1,000	9,000	1	1,000	1,000	1,000	1,000	1,000	1,000	1,000
OpenChain	1,000	9,000	1,000	1	1,000	1,000	1,000	1,000	1,000	1,000
BigchainDB	1,000	9,000	1,000	1,000	1	1,000	1,000	1,000	1,000	1,000
IOTA	1,000	9,000	1,000	1,000	1,000	1	1,000	1,000	1,000	1,000
HydraChain	1,000	9,000	1,000	1,000	1,000	1,000	1	1,000	1,000	1,000
Avalanche	1,000	9,000	1,000	1,000	1,000	1,000	1,000	1	1,000	1,000
Parity	1,000	9,000	1,000	1,000	1,000	1,000	1,000	1,000	1	1,000
Kadena	1,000	9,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1
TOPLAM	9,111	82,000	9,111	9,111	9,111	9,111	9,111	9,111	9,111	9,111

Adım 4. Matrislerin normalize edilmesi: Çizelge 5.33'te verilen ikili karşılaştırma matrisindeki her bir hücre değeri ilgili sütunun toplam değerine bölünerek normalize edilmektedir. Normalize edilmiş ikili karşılaştırma matrisi Çizelge 5.34'te verilmiştir.

Çizelge 5.34. Normalize edilmiş ikili karşılaştırma matrisi – DoS & DDoS Direnci (N)

DoS & DDoS DİRENCİ	Hyperledger	Quorum	Corda	OpenChain	BigchainDB	IOTA	HydraChain	Avalanche	Parity	Kadena	Ağırlık
Hyperledger	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110
Quorum	0,012	0,012	0,012	0,012	0,012	0,012	0,012	0,012	0,012	0,012	0,012
Corda	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110
OpenChain	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110
BigchainDB	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110
IOTA	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110
HydraChain	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110
Avalanche	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110
Parity	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110
Kadena	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110
TOPLAM	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000

Adım 5. Öncelik vektörünün hesaplanması: Çizelge 5.34'te verilmiş olan normalize edilmiş matrisin "Ağırlık" başlıklı sütunu, her bir ilgili satırdaki değerlerin ortalamasını ifade etmekte olup bu ortalama değerler öncelik vektörüdür. Buna göre, seçim kriterleri öncelik vektörü Çizelge 5.35'te verilmiştir.

Çizelge 5.35. Öncelik Vektörü – DoS & DDoS Direnci (Ö)

Alternatif	Öncelik Vektörü
Hyperledger	0,110
Quorum	0,012
Corda	0,110
OpenChain	0,110
BigchainDB	0,110
IOTA	0,110
HydraChain	0,110
Avalanche	0,110
Parity	0,110
Kadena	0,110

Adım 6. Tutarlılık analizinin yapılması: İlgili tutarlılık analizi formülleri (Bkz. Eş. 2.6, 2.7 ve 2.8) kullanılarak yapılan hesaplama sonucunda elde edilen değerleri içeren, normalize edilmiş matris ile öncelik vektörünün çarpımı ile elde edilmiş olan matris Çizelge 5.36'da verilmiştir.

Çizelge 5.36. Tutarlılık analizi tablosu – DoS&DDoS direnci (NxÖ)

DoS&DDoS DİRENCİ	Hyperledger	Quorum	Corda	OpenChain	BigchainDB	IOTA	HydraChain	Avalanche	Parity	Kadena	Toplam	Ağırlık	Ağırlık (Önc. Vektörü)
Hyperledger	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	1,098	0,110	10,000
Quorum	0,012	0,012	0,012	0,012	0,012	0,012	0,012	0,012	0,012	0,012	0,122	0,012	10,000
Corda	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	1,098	0,110	10,000
OpenChain	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	1,098	0,110	10,000
BigchainDB	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	1,098	0,110	10,000
IOTA	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	1,098	0,110	10,000
HydraChain	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	1,098	0,110	10,000
Avalanche	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	1,098	0,110	10,000
Parity	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	1,098	0,110	10,000
Kadena	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	0,110	1,098	0,110	10,000
TOPLAM	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000			
Ortalama (λ_{max})												10,000	
CI [$(\lambda_{max} - n)/(n-1)$]												0	
RI (Çizelge 2.42'de yer alan Rassal Indeks değerlerinden n=10'a karşılık gelen)												1,485	
CR=CI/RI												0	
Limit												**0,10 (%10)**	
CR < Limit olduğundan tutarlıdır.													

CR değeri limit değer olan 0,10'dan küçük olduğu için karşılaştırma matrisi tutarlıdır ve sonraki işlem adımlarına devam edilebilir.

Ağ gecikmesi

Özellik	**Hyperledger**	**Quorum**	**Corda**	**OpenChain**	**BigchainDB**	**IOTA**	**HydraChain**	**Avalanche**	**Parity**	**Kadena**
Ağ gecikmesi - 7	2	1	1	1	1	2	1	2	3	1

Ağ gecikmesi, düşük olması istenen bir özellik olduğundan kriterlerin değerlendirmesinde diğer kriterlerde olduğundan farklı bir yaklaşım gösterilmektedir. Burada, "Çok düşük" ile ifade edilen gecikme için kullanılan "1" değeri en iyi ve istenen durumdur. Bu nedenle, ağ gecikmesine ilişkin karşılaştırmalarda üstünlük ya da önem derecesi belirlenirken ağ gecikmesi "1" olanların diğer platformlara daha üstün ya da önemli oldukları göz önüne

alınmalıdır. Platform alternatiflerinin "ağ gecikmesi" kriterine göre özellikleri aşağıdaki biçimdedir:

- Quorum, Corda, OpenChain, BigchainDB, HydraChain ve Kadena ağ gecikmesi "Çok düşük" olan platformlardır ve birbirlerine göre önem dereceleri eşittir.
- Hyperledger, IOTA ve Avalanche ağ gecikmesi "Düşük" olan platformlardır ve birbirlerine göre önem dereceleri eşittir.
- Parity ağ gecikmesi "Orta" olan tek platformdur.
- 1 – 5 skalasında değerlendirilmiş olan ağ gecikmesi özelliği için Quorum, Corda, OpenChain, BigchainDB, HydraChain ve Kadena;
  - Hyperledger, IOTA ve Avalanche'a göre biraz daha önemli (3),
  - Parity'ye göre ise esaslı veya güçlü önemdedir (5).
- 1 – 5 skalasında değerlendirilmiş olan ağ gecikmesi özelliği için Hyperledger, IOTA ve Avalanche;
  - Parity'ye göre biraz daha önemlidir (3).

Verilen bu bilgilere göre ağ gecikmesi kriterine göre alternatiflerin birbirlerine göre önem derecelerini gösteren ikili karşılaştırma matrisi Çizelge 5.37'de verilmiştir.

Çizelge 5.37. Ağ gecikmesi kriterine göre alternatiflerin ikili karşılaştırma matrisi

AĞ GECİKMESİ	Hyperledger	Quorum	Corda	OpenChain	BigchainDB	IOTA	HydraChain	Avalanche	Parity	Kadena
Hyperledger	1	0,333	0,333	0,333	0,333	1,000	0,333	1,000	3,000	0,333
Quorum	3,000	1	1,000	1,000	1,000	3,000	1,000	3,000	5,000	1,000
Corda	3,000	1,000	1	1,000	1,000	3,000	1,000	3,000	5,000	1,000
OpenChain	3,000	1,000	1,000	1	1,000	3,000	1,000	3,000	5,000	1,000
BigchainDB	3,000	1,000	1,000	1,000	1	3,000	1,000	3,000	5,000	1,000
IOTA	1,000	0,333	0,333	0,333	0,333	1	0,333	1,000	3,000	0,333
HydraChain	3,000	1,000	1,000	1,000	1,000	3,000	1	3,000	5,000	1,000
Avalanche	1,000	0,333	0,333	0,333	0,333	1,000	0,333	1	3,000	0,333
Parity	0,333	0,200	0,200	0,200	0,200	0,333	0,200	0,333	1	0,200
Kadena	3,000	1,000	1,000	1,000	1,000	3,000	1,000	3,000	5,000	1
TOPLAM	21,333	7,200	7,200	7,200	7,200	21,333	7,200	21,333	40,000	7,200

Adım 4. Matrislerin normalize edilmesi: Çizelge 5.37'de verilen ikili karşılaştırma matrisindeki her bir hücre değeri ilgili sütunun toplam değerine bölünerek normalize edilmektedir. Normalize edilmiş ikili karşılaştırma matrisi Çizelge 5.38'de verilmiştir.

Çizelge 5.38. Normalize edilmiş ikili karşılaştırma matrisi - Ağ gecikmesi (N)

AĞ GECİKMESİ	Hyperledger	Quorum	Corda	OpenChain	BigchainDB	IOTA	HydraChain	Avalanche	Parity	Kadena	Ağırlık
Hyperledger	0,047	0,046	0,046	0,046	0,046	0,047	0,046	0,047	0,075	0,046	0,049
Quorum	0,141	0,139	0,139	0,139	0,139	0,141	0,139	0,141	0,125	0,139	0,138
Corda	0,141	0,139	0,139	0,139	0,139	0,141	0,139	0,141	0,125	0,139	0,138
OpenChain	0,141	0,139	0,139	0,139	0,139	0,141	0,139	0,141	0,125	0,139	0,138
BigchainDB	0,141	0,139	0,139	0,139	0,139	0,141	0,139	0,141	0,125	0,139	0,138
IOTA	0,047	0,046	0,046	0,046	0,046	0,047	0,046	0,047	0,075	0,046	0,049
HydraChain	0,141	0,139	0,139	0,139	0,139	0,141	0,139	0,141	0,125	0,139	0,138
Avalanche	0,047	0,046	0,046	0,046	0,046	0,047	0,046	0,047	0,075	0,046	0,049
Parity	0,016	0,028	0,028	0,028	0,028	0,016	0,028	0,016	0,025	0,028	0,024
Kadena	0,141	0,139	0,139	0,139	0,139	0,141	0,139	0,141	0,125	0,139	0,138
TOPLAM	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000

Adım 5. Öncelik vektörünün hesaplanması: Çizelge 5.38'de verilmiş olan normalize edilmiş matrisin "Ağırlık" başlıklı sütunu, her bir ilgili satırdaki değerlerin ortalamasını ifade etmekte olup bu ortalama değerler öncelik vektörüdür. Buna göre, seçim kriterleri öncelik vektörü Çizelge 5.39'da verilmiştir.

Çizelge 5.39. Öncelik Vektörü – Ağ gecikmesi (Ö)

Alternatif	Öncelik Vektörü
Hyperledger	0,049
Quorum	0,138
Corda	0,138
OpenChain	0,138
BigchainDB	0,138
IOTA	0,049
HydraChain	0,138
Avalanche	0,049
Parity	0,024
Kadena	0,138

Adım 6. Tutarlılık analizinin yapılması: İlgili tutarlılık analizi formülleri (Bkz. Eş. 2.6, 2.7 ve 2.8) kullanılarak yapılan hesaplama sonucunda elde edilen değerleri içeren, normalize edilmiş matris ile öncelik vektörünün çarpımı ile elde edilmiş olan matris Çizelge 5.40'ta verilmiştir.

Çizelge 5.40. Tutarlılık analizi tablosu – Ağ gecikmesi (NxÖ)

AĞ GECİKMESİ	**Hyperledger**	**Quorum**	**Corda**	**OpenChain**	**BigchainDB**	**IOTA**	**HydraChain**	**Avalanche**	**Parity**	**Kadena**	**Toplam**	**Ağrlık**	**Ağrlık (Önc. Vektörü)**
Hyperledger	0,049	0,046	0,046	0,046	0,046	0,049	0,046	0,049	0,072	0,046	0,496	0,049	10,045
Quorum	0,148	0,138	0,138	0,138	0,138	0,148	0,138	0,148	0,119	0,138	1,391	0,138	10,082
Corda	0,148	0,138	0,138	0,138	0,138	0,148	0,138	0,148	0,119	0,138	1,391	0,138	10,082
OpenChain	0,148	0,138	0,138	0,138	0,138	0,148	0,138	0,148	0,119	0,138	1,391	0,138	10,082
BigchainDB	0,148	0,138	0,138	0,138	0,138	0,148	0,138	0,148	0,119	0,138	1,391	0,138	10,082
IOTA	0,049	0,046	0,046	0,046	0,046	0,049	0,046	0,049	0,072	0,046	0,496	0,049	10,045
HydraChain	0,148	0,138	0,138	0,138	0,138	0,148	0,138	0,148	0,119	0,138	1,391	0,138	10,082
Avalanche	0,049	0,046	0,046	0,046	0,046	0,049	0,046	0,049	0,072	0,046	0,496	0,049	10,045
Parity	0,016	0,028	0,028	0,028	0,028	0,016	0,028	0,016	0,024	0,028	0,239	0,024	10,012
Kadena	0,148	0,138	0,138	0,138	0,138	0,148	0,138	0,148	0,119	0,138	1,391	0,138	10,082
TOPLAM	1,053	0,994	0,994	0,994	0,994	1,053	0,994	1,053	0,954	0,994			
Ortalama (λ_{max})													10,064
CI $[(\lambda_{max} - n)/(n-1)]$													0,007064639
RI (Çizelge 2.42'de yer alan Rassal Indeks değerlerinden n=10'a karşılık gelen)													1,485
CR=CI/RI													0,004757333
Limit													**0,10 (%10)**
CR < Limit olduğundan tutarlıdır.													

CR değeri limit değer olan 0,10'dan küçük olduğu için karşılaştırma matrisi tutarlıdır ve sonraki işlem adımlarına devam edilebilir.

İşlem hacmi

Özellik	**Hyperledger**	**Quorum**	**Corda**	**OpenChain**	**BigchainDB**	**IOTA**	**HydraChain**	**Avalanche**	**Parity**	**Kadena**
İşlem hacmi (saniyede işlem sayısı) - 8	3	2	5	5	2	4	2	3	5	4

Platform alternatiflerinin "işlem hacmi" kriterine göre özellikleri aşağıdaki biçimdedir:

- Corda, OpenChain ve Parity işlem hacmi "Çok yüksek" olan platformlardır ve birbirlerine göre önem dereceleri eşittir.
- IOTA ve Kadena işlem hacmi "Yüksek" olan platformlardır ve birbirlerine göre önem dereceleri eşittir.

- Hyperledger ve Avalanche işlem hacmi "Orta" olan platformlardır ve birbirlerine göre önem dereceleri eşittir.
- Quorum, BigchainDB ve HydraChain işlem hacmi "Orta" olan platformlardır ve birbirlerine göre önem dereceleri eşittir.
- İşlem hacmi "Çük düşük" olan platform bulunmamaktadır.
- 1 – 5 skalasında değerlendirilmiş olan işlem hacmi özelliği için Corda, OpenChain ve Parity;
  - IOTA ve Kadena'ya göre biraz daha önemli (3),
  - Hyperledger ve Avalanche'a göre esaslı veya güçlü önemde (5),
  - Quorum, BigchainDB ve HydraChain'e göre ise çok güçlü önemdedir (7).
- 1 – 5 skalasında değerlendirilmiş olan işlem hacmi özelliği için IOTA ve Kadena;
  - Hyperledger ve Avalanche'a göre biraz daha önemli (3),
  - Quorum, BigchainDB ve HydraChain'e göre ise esaslı veya güçlü önemdedir (5).
- 1 – 5 skalasında değerlendirilmiş olan işlem hacmi özelliği için Hyperledger ve Avalanche;
  - Quorum, BigchainDB ve HydraChain'e göre biraz daha önemlidir (3).

Verilen bu bilgilere göre işlem hacmi kriterine göre alternatiflerin birbirlerine göre önem derecelerini gösteren ikili karşılaştırma matrisi Çizelge 5.41'de verilmiştir.

Çizelge 5.41. İşlem hacmi kriterine göre alternatiflerin ikili karşılaştırma matrisi

İŞLEM HACMİ	Hyperledger	Quorum	Corda	OpenChain	BigchainDB	IOTA	HydraChain	Avalanche	Parity	Kadena
Hyperledger	1	3,000	0,500	0,200	3,000	0,333	3,000	1,000	0,200	0,333
Quorum	0,333	1	0,143	0,143	1,000	0,200	1,000	0,333	0,143	0,200
Corda	2,000	7,000	1	1,000	7,000	3,000	7,000	5,000	1,000	3,000
OpenChain	5,000	7,000	1,000	1	7,000	3,000	7,000	5,000	1,000	3,000
BigchainDB	0,333	1,000	0,143	0,143	1	0,200	1,000	0,333	0,143	0,200
IOTA	3,000	5,000	0,333	0,333	5,000	1	5,000	3,000	0,333	1,000
HydraChain	0,333	1,000	0,143	0,143	1,000	0,200	1	0,333	0,143	0,200
Avalanche	1,000	3,000	0,200	0,200	3,000	0,333	3,000	1	0,200	0,333
Parity	5,000	7,000	1,000	1,000	7,000	3,000	7,000	5,000	1	3,000
Kadena	3,000	5,000	0,333	0,333	5,000	1,000	5,000	3,000	0,333	1
TOPLAM	21,000	40,000	4,795	4,495	40,000	12,267	40,000	24,000	4,495	12,267

Adım 4. Matrislerin normalize edilmesi: Çizelge 5.41'de verilen ikili karşılaştırma matrisindeki her bir hücre değeri ilgili sütunun toplam değerine bölünerek normalize edilmektedir. Normalize edilmiş ikili karşılaştırma matrisi Çizelge 5.42'de verilmiştir.

Çizelge 5.42. Normalize edilmiş ikili karşılaştırma matrisi - İşlem hacmi (N)

İŞLEM HACMİ	Hyperledger	Quorum	Corda	OpenChain	BigchainDB	IOTA	HydraChain	Avalanche	Parity	Kadena	Ağırlık
Hyperledger	0,048	0,075	0,104	0,044	0,075	0,027	0,075	0,042	0,044	0,027	0,056
Quorum	0,016	0,025	0,030	0,032	0,025	0,016	0,025	0,014	0,032	0,016	0,023
Corda	0,095	0,175	0,209	0,222	0,175	0,245	0,175	0,208	0,222	0,245	0,197
OpenChain	0,238	0,175	0,209	0,222	0,175	0,245	0,175	0,208	0,222	0,245	0,211
BigchainDB	0,016	0,025	0,030	0,032	0,025	0,016	0,025	0,014	0,032	0,016	0,023
IOTA	0,143	0,125	0,070	0,074	0,125	0,082	0,125	0,125	0,074	0,082	0,102
HydraChain	0,016	0,025	0,030	0,032	0,025	0,016	0,025	0,014	0,032	0,016	0,023
Avalanche	0,048	0,075	0,042	0,044	0,075	0,027	0,075	0,042	0,044	0,027	0,050
Parity	0,238	0,175	0,209	0,222	0,175	0,245	0,175	0,208	0,222	0,245	0,211
Kadena	0,143	0,125	0,070	0,074	0,125	0,082	0,125	0,125	0,074	0,082	0,102
TOPLAM	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000

Adım 5. Öncelik vektörünün hesaplanması: Çizelge 5.42'de verilmiş olan normalize edilmiş matrisin "Ağırlık" başlıklı sütunu, her bir ilgili satırdaki değerlerin ortalamasını ifade etmekte olup bu ortalama değerler öncelik vektörüdür. Buna göre, seçim kriterleri öncelik vektörü Çizelge 5.43'te verilmiştir.

Çizelge 5.43. Öncelik Vektörü – İşlem hacmi (Ö)

Alternatif	**Öncelik Vektörü**
Hyperledger	0,056
Quorum	0,023
Corda	0,197
OpenChain	0,211
BigchainDB	0,023
IOTA	0,102
HydraChain	0,023
Avalanche	0,050
Parity	0,211
Kadena	0,102

Adım 6. Tutarlılık analizinin yapılması: İlgili tutarlılık analizi formülleri (Bkz. Eş. 2.6, 2.7 ve 2.8) kullanılarak yapılan hesaplama sonucunda elde edilen değerleri içeren, normalize edilmiş matris ile öncelik vektörünün çarpımı ile elde edilmiş olan matris Çizelge 5.44'te verilmiştir.

Çizelge 5.44. Tutarlılık analizi tablosu - İşlem hacmi (NxÖ)

İŞLEM HACMİ	**Hyperledger**	**Quorum**	**Corda**	**OpenChain**	**BigchainDB**	**IOTA**	**HydraChain**	**Avalanche**	**Parity**	**Kadena**	**Toplam**	**Ağırlık**	**Ağırlık (Önc. Vektörü)**
Hyperledger	0,056	0,069	0,099	0,042	0,069	0,034	0,069	0,050	0,042	0,034	0,565	0,056	10,058
Quorum	0,019	0,023	0,028	0,030	0,023	0,020	0,023	0,017	0,030	0,020	0,234	0,023	10,146
Corda	0,112	0,162	0,197	0,211	0,162	0,307	0,162	0,250	0,211	0,307	2,081	0,197	10,556
OpenChain	0,281	0,162	0,197	0,211	0,162	0,307	0,162	0,250	0,211	0,307	2,249	0,211	10,640
BigchainDB	0,019	0,023	0,028	0,030	0,023	0,020	0,023	0,017	0,030	0,020	0,234	0,023	10,146
IOTA	0,169	0,115	0,066	0,070	0,115	0,102	0,115	0,150	0,070	0,102	1,076	0,102	10,509
HydraChain	0,019	0,023	0,028	0,030	0,023	0,020	0,023	0,017	0,030	0,020	0,234	0,023	10,146
Avalanche	0,056	0,069	0,039	0,042	0,069	0,034	0,069	0,050	0,042	0,034	0,506	0,050	10,134
Parity	0,281	0,162	0,197	0,211	0,162	0,307	0,162	0,250	0,211	0,307	2,249	0,211	10,640
Kadena	0,169	0,115	0,066	0,070	0,115	0,102	0,115	0,150	0,070	0,102	1,076	0,102	10,509
TOPLAM	1,180	0,923	0,945	0,950	0,923	1,256	0,923	1,198	0,950	1,256			
Ortalama (λ_{max})													10,348
CI $[(\lambda_{max} - n)/(n-1)]$													0,038712508
RI (Çizelge 2.42'de yer alan Rassal Indeks değerlerinden n=10'a karşılık gelen)													1,485
CR=CI/RI													0,026069029
Limit													**0,10 (%10)**
CR < Limit olduğundan tutarlıdır.													

CR değeri limit değer olan 0,10'dan küçük olduğu için karşılaştırma matrisi tutarlıdır ve sonraki işlem adımlarına devam edilebilir.

İşlem hızı

Özellik	**Hyperledger**	**Quorum**	**Corda**	**OpenChain**	**BigchainDB**	**IOTA**	**HydraChain**	**Avalanche**	**Parity**	**Kadena**
İşlem hızı - 9	3	5	5	5	4	3	3	3	3	2

Platform alternatiflerinin "işlem hızı" kriterine göre özellikleri aşağıdaki biçimdedir:

- Quorum, Corda ve OpenChain platformları işlem hızı "Çok yüksek" olan platformlardır ve birbirlerine göre önem dereceleri eşittir.
- BigchainDB platformu işlem hızı "Yüksek" olan tek platformdur.
- Hyperledger, IOTA, HydraChain, Avalanche ve Parity işlem hızı "Orta" olan platformlardır ve birbirlerine göre önem dereceleri eşittir.
- Kadena işlem hızı "Düşük" olan tek platformdur.
- 1–5 skalasında değerlendirilmiş olan işlem hızı özelliği için Quorum, Corda, OpenChain;
  - BigchainDB'ye göre biraz daha önemli (3),
  - Hyperledger, IOTA, HydraChain, Avalanche ve Parity'ye göre esaslı veya güçlü önemde (5),
  - Kadena'ya göre ise çok güçlü önemdedir (7).
- 1 – 5 skalasında değerlendirilmiş olan işlem hızı özelliği için BigchainDB;
  - Hyperledger, IOTA, HydraChain, Avalanche, Parity'ye göre biraz daha önemli (3),
  - Kadena'ya göre ise esaslı veya güçlü önemdedir (5).
- 1 – 5 skalasında değerlendirilmiş olan işlem hızı özelliği için Hyperledger, IOTA, HydraChain, Avalanche ve Parity;
  - Kadena'ya göre biraz daha önemlidir (3).

Verilen bu bilgilere göre işlem hızı kriterine göre alternatiflerin birbirlerine göre önem derecelerini gösteren ikili karşılaştırma matrisi Çizelge 5.45'de verilmiştir.

Çizelge 5.45. İşlem hızı kriterine göre alternatiflerin ikili karşılaştırma matrisi

İŞLEM HIZI	Hyperledger	Quorum	Corda	OpenChain	BigchainDB	IOTA	HydraChain	Avalanche	Parity	Kadena
Hyperledger	1	0,200	0,200	0,200	0,333	1,000	1,000	1,000	1,000	3,000
Quorum	5,000	1	1,000	1,000	3,000	5,000	5,000	5,000	5,000	7,000
Corda	5,000	1,000	1	1,000	3,000	5,000	5,000	5,000	5,000	7,000
OpenChain	5,000	1,000	1,000	1	3,000	5,000	5,000	5,000	5,000	7,000
BigchainDB	3,000	0,333	0,333	0,333	1	3,000	3,000	3,000	3,000	5,000
IOTA	1,000	0,200	0,200	0,200	0,333	1	1,000	1,000	1,000	3,000
HydraChain	1,000	0,200	0,200	0,200	0,333	1,000	1	1,000	1,000	3,000
Avalanche	1,000	0,200	0,200	0,200	0,333	1,000	1,000	1	1,000	3,000
Parity	1,000	0,200	0,200	0,200	0,333	1,000	1,000	1,000	1	3,000
Kadena	0,333	0,143	0,143	0,143	0,200	0,333	0,333	0,333	0,333	1
TOPLAM	23,333	4,476	4,476	4,476	11,867	23,333	23,333	23,333	23,333	42,000

Adım 4. Matrislerin normalize edilmesi: Çizelge 5.45'te verilen ikili karşılaştırma matrisindeki her bir hücre değeri ilgili sütunun toplam değerine bölünerek normalize edilmektedir. Normalize edilmiş ikili karşılaştırma matrisi Çizelge 5.46'da verilmiştir.

Çizelge 5.46. Normalize edilmiş ikili karşılaştırma matrisi – İşlem hızı (N)

İŞLEM HIZI	Hyperledger	Quorum	Corda	OpenChain	BigchainDB	IOTA	HydraChain	Avalanche	Parity	Kadena	Ağırlık
Hyperledger	0,043	0,045	0,045	0,045	0,028	0,043	0,043	0,043	0,043	0,071	0,045
Quorum	0,214	0,223	0,223	0,223	0,253	0,214	0,214	0,214	0,214	0,167	0,216
Corda	0,214	0,223	0,223	0,223	0,253	0,214	0,214	0,214	0,214	0,167	0,216
OpenChain	0,214	0,223	0,223	0,223	0,253	0,214	0,214	0,214	0,214	0,167	0,216
BigchainDB	0,129	0,074	0,074	0,074	0,084	0,129	0,129	0,129	0,129	0,119	0,107
IOTA	0,043	0,045	0,045	0,045	0,028	0,043	0,043	0,043	0,043	0,071	0,045
HydraChain	0,043	0,045	0,045	0,045	0,028	0,043	0,043	0,043	0,043	0,071	0,045
Avalanche	0,043	0,045	0,045	0,045	0,028	0,043	0,043	0,043	0,043	0,071	0,045
Parity	0,043	0,045	0,045	0,045	0,028	0,043	0,043	0,043	0,043	0,071	0,045
Kadena	0,014	0,032	0,032	0,032	0,017	0,014	0,014	0,014	0,014	0,024	0,021
TOPLAM	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000

Adım 5. Öncelik vektörünün hesaplanması: Çizelge 5.46'da verilmiş olan normalize edilmiş matrisin "Ağırlık" başlıklı sütunu, her bir ilgili satırdaki değerlerin ortalamasını ifade etmekte olup bu ortalama değerler öncelik vektörüdür. Buna göre, seçim kriterleri öncelik vektörü Çizelge 5.47'de verilmiştir.

Çizelge 5.47. Öncelik Vektörü – İşlem hızı (Ö)

Alternatif	**Öncelik Vektörü**
Hyperledger	0,045
Quorum	0,216
Corda	0,216
OpenChain	0,216
BigchainDB	0,107
IOTA	0,045
HydraChain	0,045
Avalanche	0,045
Parity	0,045
Kadena	0,021

Adım 6. Tutarlılık analizinin yapılması: İlgili tutarlılık analizi formülleri (Bkz. Eş. 2.6, 2.7 ve 2.8) kullanılarak yapılan hesaplama sonucunda elde edilen değerleri içeren, normalize edilmiş matris ile öncelik vektörünün çarpımı ile elde edilmiş olan matris Çizelge 5.48'de verilmiştir.

Çizelge 5.48. Tutarlılık analizi tablosu - İşlem hızı (NxÖ)

İŞLEM HIZI	**Hyperledger**	**Quorum**	**Corda**	**OpenChain**	**BigchainDB**	**IOTA**	**HydraChain**	**Avalanche**	**Parity**	**Kadena**	**Toplam**	**Ağırlık**	**Ağırlık (Önc. Vektörü)**
Hyperledger	0,045	0,043	0,043	0,043	0,036	0,045	0,045	0,045	0,045	0,062	0,452	0,045	10,084
Quorum	0,224	0,216	0,216	0,216	0,321	0,224	0,224	0,224	0,224	0,145	2,234	0,216	10,339
Corda	0,224	0,216	0,216	0,216	0,321	0,224	0,224	0,224	0,224	0,145	2,234	0,216	10,339
OpenChain	0,224	0,216	0,216	0,216	0,321	0,224	0,224	0,224	0,224	0,145	2,234	0,216	10,339
BigchainDB	0,134	0,072	0,072	0,072	0,107	0,134	0,134	0,134	0,134	0,104	1,099	0,107	10,273
IOTA	0,045	0,043	0,043	0,043	0,036	0,045	0,045	0,045	0,045	0,062	0,452	0,045	10,084
HydraChain	0,045	0,043	0,043	0,043	0,036	0,045	0,045	0,045	0,045	0,062	0,452	0,045	10,084
Avalanche	0,045	0,043	0,043	0,043	0,036	0,045	0,045	0,045	0,045	0,062	0,452	0,045	10,084
Parity	0,045	0,043	0,043	0,043	0,036	0,045	0,045	0,045	0,045	0,062	0,452	0,045	10,084
Kadena	0,015	0,031	0,031	0,031	0,021	0,015	0,015	0,015	0,015	0,021	0,209	0,021	10,077
TOPLAM	1,045	0,967	0,967	0,967	1,269	1,045	1,045	1,045	1,045	0,873			
Ortalama (λ_{max})													10,178
CI $[(\lambda_{max} - n)/(n-1)]$													0,019824149
RI (Çizelge 2.42'de yer alan Rassal Indeks değerlerinden n=10'a karşılık gelen)													1,485
CR=CI/RI													0,013349595
Limit													**0,10 (%10)**
CR < Limit olduğundan tutarlıdır.													

CR değeri limit değer olan 0,10'dan küçük olduğu için karşılaştırma matrisi tutarlıdır ve sonraki işlem adımlarına devam edilebilir.

Token kullanımı

Özellik	**Hyperledger**	**Quorum**	**Corda**	**OpenChain**	**BigchainDB**	**IOTA**	**HydraChain**	**Avalanche**	**Parity**	**Kadena**
Token kullanımı - 10	2	1	1	1	1	1	1	1	1	1

Token kullanımı özelliği için seçenekler yalnızca evet (1) ve hayırdır (2). Token kullanımı sadece Hyperledger için "hayır" olarak seçilmiştir. Hyperledger'in Fabric versiyonu için her ne kadar kapalı devre token kullanımı mümkün olsa da, birden fazla çeşide sahip olduğu göz önüne alınarak bu platform için token kullanımının kısıtlı olduğu değerlendirilmiştir. Buna göre;

- Quorum, Corda, OpenChain, BigchainDB, IOTA, HydraChain, Avalanche, Parity ve Kadena platformlarının önem dereceleri birbirine eşittir. Bu platformların Hyperledger'a göre çok güçlü önemdedir (7).

Verilen bu bilgilere göre token kullanımı kriterine göre alternatiflerin birbirlerine göre önem derecelerini gösteren ikili karşılaştırma matrisi Çizelge 5.49'da verilmiştir.

Çizelge 5.49. Token kullanımı kriterine göre alternatiflerin ikili karşılaştırma matrisi

TOKEN KULLANIMI	Hyperledger	Quorum	Corda	OpenChain	BigchainDB	IOTA	HydraChain	Avalanche	Parity	Kadena
Hyperledger	1	0,143	0,143	0,143	0,143	0,143	0,143	0,143	0,143	0,143
Quorum	7,000	1	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000
Corda	7,000	1,000	1	1,000	1,000	1,000	1,000	1,000	1,000	1,000
OpenChain	7,000	1,000	1,000	1	1,000	1,000	1,000	1,000	1,000	1,000
BigchainDB	7,000	1,000	1,000	1,000	1	1,000	1,000	1,000	1,000	1,000
IOTA	7,000	1,000	1,000	1,000	1,000	1	1,000	1,000	1,000	1,000
HydraChain	7,000	1,000	1,000	1,000	1,000	1,000	1	1,000	1,000	1,000
Avalanche	7,000	1,000	1,000	1,000	1,000	1,000	1,000	1	1,000	1,000
Parity	7,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1	1,000
Kadena	7,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1
TOPLAM	64,000	9,143	9,143	9,143	9,143	9,143	9,143	9,143	9,143	9,143

Adım 4. Matrislerin normalize edilmesi: Çizelge 5.49'da verilen ikili karşılaştırma matrisindeki her bir hücre değeri ilgili sütunun toplam değerine bölünerek normalize edilmektedir. Normalize edilmiş ikili karşılaştırma matrisi Çizelge 5.50'de verilmiştir.

Çizelge 5.50. Normalize edilmiş ikili karşılaştırma matrisi - Token kullanımı (N)

TOKEN KULLANIMI	Hyperledger	Quorum	Corda	OpenChain	BigchainDB	IOTA	HydraChain	Avalanche	Parity	Kadena	Ağırlık
Hyperledger	0,016	0,016	0,016	0,016	0,016	0,016	0,016	0,016	0,016	0,016	0,016
Quorum	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109
Corda	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109
OpenChain	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109
BigchainDB	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109
IOTA	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109
HydraChain	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109
Avalanche	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109
Parity	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109
Kadena	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109
TOPLAM	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000

Adım 5. Öncelik vektörünün hesaplanması: Çizelge 5.50'de verilmiş olan normalize edilmiş matrisin "Ağırlık" başlıklı sütunu, her bir ilgili satırdaki değerlerin ortalamasını ifade etmekte olup bu ortalama değerler öncelik vektörüdür. Buna göre, seçim kriterleri öncelik vektörü Çizelge 5.51'de verilmiştir.

Çizelge 5.51. Öncelik Vektörü – Token kullanımı (Ö)

Alternatif	Öncelik Vektörü
Hyperledger	0,016
Quorum	0,109
Corda	0,109
OpenChain	0,109
BigchainDB	0,109
IOTA	0,109
HydraChain	0,109
Avalanche	0,109
Parity	0,109
Kadena	0,109

Adım 6. Tutarlılık analizinin yapılması: İlgili tutarlılık analizi formülleri (Bkz. Eş. 2.6, 2.7 ve 2.8) kullanılarak yapılan hesaplama sonucunda elde edilen değerleri içeren, normalize edilmiş matris ile öncelik vektörünün çarpımı ile elde edilmiş olan matris Çizelge 5.52'de verilmiştir.

Çizelge 5.52. Tutarlılık analizi tablosu – Token kullanımı (NxÖ)

İŞLEM HIZI	Hyperledger	Quorum	Corda	OpenChain	BigchainDB	IOTA	HydraChain	Avalanche	Parity	Kadena	Toplam	Ağırlık	Ağırlık (Önc. Vektörü)
Hyperledger	0,016	0,016	0,016	0,016	0,016	0,016	0,016	0,016	0,016	0,016	0,156	0,016	10,000
Quorum	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	1,094	0,109	10,000
Corda	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	1,094	0,109	10,000
OpenChain	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	1,094	0,109	10,000
BigchainDB	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	1,094	0,109	10,000
IOTA	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	1,094	0,109	10,000
HydraChain	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	1,094	0,109	10,000
Avalanche	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	1,094	0,109	10,000
Parity	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	1,094	0,109	10,000
Kadena	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	0,109	1,094	0,109	10,000
TOPLAM	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000			
Ortalama (λ_{max})													10,000
CI $[(\lambda_{max} - n)/(n-1)]$													0
RI (Çizelge 2.42'de yer alan Rassal Indeks değerlerinden n=10'a karşılık gelen)													1,485
CR=CI/RI													0
Limit													**0,10 (%10)**
CR < Limit olduğundan tutarlıdır.													

CR değeri limit değer olan 0,10'dan küçük olduğu için karşılaştırma matrisi tutarlıdır ve sonraki işlem adımlarına devam edilebilir.

5.4.3. Çözüm alternatiflerinin bu özelliklere göre değerlendirilerek öncelik sırasına göre sıralanması

Son adımda, nihai sonuca ulaşmak için Çizelge 5.53'te verilmiş olan alternatiflerin kriterlere göre ağırlıklarının matrisi ile, seçim kriterlerinin ikili karşılaştırma matrisinden (Bkz. Çizelge 5.12) elde edilen öncelik vektörü çarpılır. Çizelge 5.53'te verilmiş olan matris alternatiflerin kriterlere göre karşılaştırma matrislerinden elde edilen öncelik vektörlerinin (Bkz. Çizelgeler 5.17, 5.21, 5.25, 5.27, 5.31, 5.35, 5.39, 5.43, 5.47 ve 5.51) bir araya getirilmesi ile oluşturulmaktadır.

Çizelge 5.53. Alternatiflerin kriterlere göre karşılaştırma öncelik vektörleri

Kriter / Alternatif	Güvenilirlik	Olgunluk	Popülarite	Sybil direnci	Kuantum direnci	DoS& DDoS direnci	Ağ gecikmesi	İşlem hacmi	İşlem hızı	Token kullanımı
Hyperledger	0,312	0,295	0,273	0,100	0,014	0,110	0,049	0,056	0,045	0,016
Quorum	0,162	0,142	0,115	0,100	0,014	0,012	0,138	0,023	0,216	0,109
Corda	0,162	0,142	0,115	0,100	0,122	0,110	0,138	0,197	0,216	0,109
OpenChain	0,028	0,058	0,044	0,100	0,122	0,110	0,138	0,211	0,216	0,109
BigchainDB	0,070	0,142	0,044	0,100	0,122	0,110	0,138	0,023	0,107	0,109
IOTA	0,070	0,058	0,115	0,100	0,122	0,110	0,049	0,102	0,045	0,109
HydraChain	0,028	0,025	0,044	0,100	0,122	0,110	0,138	0,023	0,045	0,109
Avalanche	0,070	0,058	0,115	0,100	0,122	0,110	0,049	0,050	0,045	0,109
Parity	0,070	0,025	0,115	0,100	0,122	0,110	0,024	0,211	0,045	0,109
Kadena	0,028	0,058	0,022	0,100	0,122	0,110	0,138	0,102	0,021	0,109
TOPLAM	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000	1,000

Nihai öncelik sıralaması, Çizelge 5.53'te verilmiş olan matris ile kriterlerin birbirleri ile karşılaştırma matrisinden elde edilmiş olan kriterler öncelik vektörünün (Bkz. Çizelge 5.12) çarpımı ile elde edilmektedir. Yani, bu çarpım sonucu her bir karar alternatifinin seçim için kullanılacak ağırlığını vermektedir. Elde edilen ağırlık vektörü Çizelge 5.54'te verilmiştir.

Çizelge 5.54. Karar alternatifleri öncelik sırası

Ağırlık	Platform	Öncelik sırası		Önceliğe göre sıralama
0,220	Hyperledger	1		Hyperledger
0,123	Quorum	3		Corda
0,141	Corda	2		Quorum
0,071	OpenChain	8		BigchainDB
0,091	BigchainDB	4		IOTA
0,083	IOTA	5		Avalanche
0,053	HydraChain	10		Parity
0,081	Avalanche	6		OpenChain
0,079	Parity	7		Kadena
0,058	Kadena	9		HydraChain

Çizelge 5.54'te verilmiş olan sonuca göre, öncelik değeri 0,220 ile en yüksek olan Hyperledger kullanım alanı için en uygun tercihtir. İkinci sıradaki alternatif ise Corda platformudur.

5.5. Adım 5. Teknoloji Seçimi ve Sistem Tasarımı

Önceki adımlarda toplanan bilgiler, gerçekleştirilen hesaplamaların sonuçları ve süreç özellikleri dikkate alınarak blokzincir teknolojisini kullanan sistemin tasarımı gerçekleştirilmektedir. Bu adımda, süreç blokzincir kullanımına uygun biçimde yeniden tasarlanmakta, bu tasarımda kullanılacak olan blokzincir platformunun özellikleri listelenmektedir.

Modelin uygulanması için kullanılan ihale süreci Kamu İhale Kanunu'na tabi olmayan bir kurum tarafından yürütülen işlem adımlarını içermektedir. Sürecin mevcut işleyişi Ek-2'de verilmiş olan Süreç Bilgi Toplama Formu ile temin edilmiş, formun 8. Sorusuna verilmiş olan cevapta sürecin 15 adımı süreçte rol alan tarafların rolleri ile birlikte gösterilmiştir.

5.5.1. Sürecin blokzincir kullanımına uygun biçimde tasarlanması

Süreçte rol alan taraflar ve rolleri

Sürecin mevcut hali ile yeni tasarlanmış halinde rol alan taraflar hemen hemen aynı olmakla birlikte, bazı roller yerine akıllı sözleşmeler kullanılabilmektedir. Aşağıda verilmiş olan Çizelge 5.55'te sürecin mevcut halinde rol alan taraflar ile bunların blokzincir kullanım durumundaki karşılıkları ve rolleri verilmiştir.

Çizelge 5.55. Süreçte rol alan taraflar ve rolleri

	Mevcut	**Yeni**	**İşlevi ve açıklamalar**	**Gösterim**
1	İstekli(ler)	İstekli(ler)	Teklif vermek üzere ihale dokümanlarını alma şartlarını taşıyan ve doküman almak üzere başvuran firmalar	$İ_i$
2	Yüklenici adayları	Aday(lar)	Teklif verme şartlarını taşıyan ve ilan edilen süre içinde tekliflerini sunan firmalar	A_i
3	Yüklenici	Yüklenici	Teklif değerlendirme sonucuna göre ihaleyi kazanan firma	Y
4	Proje Birimi	Proje Birimi kullanıcısı – Akıllı Sözleşme	İhale dokümanlarının teslim edileceği isteklilerin uygunluğunu kontrol etmekten sorumlu görevli (İhale Birimi Kullanıcısı ile aynı role sahip olup bu rol de akıllı sözleşme ile yürütülebilecektir) Aynı zamanda ihale ilanının hazırlanmasından ve onaya sunulmasından da sorumludur.	PBK_i

	Mevcut	Yeni	İşlevi ve açıklamalar	Gösterim
5	-	Belge kontrol ve teslim görevlisi - Akıllı Sözleşme	İhale dokümanlarını uygun şartları taşıyan isteklilere teslim eden (teklif değerlendirme heyeti oluşturulmadan önce) ihale birimi kullanıcısı	$BKTG_i$
6	-	Sistem Yöneticisi	Kullanıcı kaydını alan, sistem kullanıcılarını ve anahtarları oluşturan, sitemi yöneten idare kullanıcısı	SY_i
7	Bilgi İşlem Birimi	Bilgi İşlem Kullanıcısı	İhale ilanının duyurulması, ihale dokümanlarının yetkili kullanıcılar tarafından indirilmeye hazır hale getirilmesi ve teknik destekten sorumlu kullanıcı	$Bİ_i$
8	İhale Birimi	İhale Birimi Kullanıcısı	İhalenin ve ilanının idari ve mali açıdan uygunluğunu değerlendiren, ihale sonucu konusunda sonraki mali işlemler için bilgi verilen ihale birimi kullanıcısı	$İBK_i$
9	Teklif Değerlendirme Heyeti başkanı	Teklif Değerlendirme Heyeti başkanı	Teklif değerlendirme faaliyetlerine başkanlık eden kullanıcı	TDHB
10	Teklif Değerlendirme Heyeti üyeleri	Teklif Değerlendirme Heyeti üyeleri	Teklifleri inceleyen, değerlendiren, puanlayan, soru ve cevap faaliyetlerini yürüten kullanıcılar	$TDHÜ_i$
11	Proje Yöneticisi	Proje Yöneticisi – Akıllı Sözleşme	Teklif değerlendirme planını, sonucunu vb. süreç içi adımları onaylayan kullanıcı	PY
12	Üst Yönetici	Üst Yönetici	Teklif değerlendirme sonucunu ve ihale kararını onaylayan kullanıcı	ÜY

Sistem, her ne kadar konsorsiyum blokzincir yapısına benzese de, dış kullanıcıların yetkilendirmesi İdare tarafından yapıldığından ve dış kullanıcılar karar mekanizmasında rol almadığından bir özel blokzincir yapısındadır. Sistemdeki roller aşağıdaki biçimdedir:

1) Sistem Yöneticisi: Yönetici, sistemin yönetiminden ve her bir teklif projesi için ihale dokümanı alan ve teklif veren kullanıcıların ve İdare kullanıcılarını içeren görevlerin oluşturulmasından sorumludur.
2) Bilgi İşlem Kullanıcısı: Kullanıcılara teknik destek sağlamakla sorumlu olup sistem içerisinde test kullanıcısı dışında aktif bir rolü bulunmamaktadır.
3) Belge Kontrol ve Teslim Görevlisi: Proje birimi tarafından gönderilen ihale dokümanlarının teslimi için istekli kullanıcılarının uygun şartları sağlayıp sağlamadığını kontrol etmekle sorumludur. Yetki belgesi, gizlilik taahhüdü ve ihale dokümanının satın alındığına dair ödeme bilgisi gibi standart kontrolleri yaptığından bu rol bir akıllı sözleşme tarafından yürütülebilecektir.
4) Proje birimi kullanıcısı: İhale birimi kullanıcısı (Belge Kontrol ve Teslim Görevlisi) ile benzer biçimde, ihale dokümanlarının teslim edileceği isteklilerin uygunluğunu kontrol etmekten sorumludur. Benzer biçimde, bu rol de akıllı sözleşme ile yürütülebilecektir.
5) Teklif Değerlendirme Heyeti üyeleri: Başkan ve üyeler olmak üzere iki tiptir. Tekliflerin teslim alınması (uygun biçimde ve zamanda), değerlendirilmesi ve değerlendirme sonuçlarının raporlanmasından sorumludur. Başkan ve üyelere farklı yetki ve sorumluluklar atanabilmektedir.

6) Teklif Değerlendirme Heyeti başkanı: Teklif Değerlendirme faaliyetlerine başkanlık eden, heyet üyelerinin puanlamalarını kontrol eden, kendisi de aynı zamanda puanlama yapan, puanlama sonuçlarını konsolide ederek değerlendirme sonucunu hazırlayan kullanıcıdır. Bu sorumlulukların büyük kısmı akıllı sözleşmeler ile sağlanabileceğinden akıllı sözleşme kullanılması durumunda bu role gereksinim duyulmayacaktır.
7) Proje Yöneticisi: Teklif Değerlendirme Planının ve Teklif Değerlendirme Heyetince yapılan değerlendirmelerin kontrol edilerek onaylanmasından sorumludur. Bu kontrol ve onaylar akıllı sözleşmeler ile sağlanabileceğinden akıllı sözleşme kullanılması durumunda bu role gereksinim duyulmayacaktır.
8) Üst Yönetici: Teklif Değerlendirme Sonuç Raporunun nihai onay için gönderildiği makam olup ihale sonucunun onaylanmasından sorumludur.
9) İstekli(ler): İhale dokümanlarını alma yetkisi bulunan, henüz teklif vermemiş olan firmalar istekli olarak adlandırılmaktadır. İhale dokümanı almak için davet edilme, doküman ücretini yatırma veya belirlenecek bazı özel şartları taşıma gibi koşullar belirlenmişse, isteklilere doküman teslimi için tüm bu şartlar kontrol edilir.
10) Aday(lar): İhale dokümanı alarak teklif sunan firmalardır. Tekliflerin sunulabilmesi için gerekli şartları (belirtilen zamandan önce teklifin sunulması, ihale dokümanlarında belirtilen vazgeçilmez şartların karşılanması, yasaklılık kararının bulunmaması gibi) taşıyan adayların teklifleri kabul edilir.
11) Yüklenici: Değerlendirme sonucunda teklifi uygun bulunarak seçilen firmayı ifade etmektedir. Mutlaka adaylardan biri olmalıdır.
12) İhale Onay Makamı: Üst Yönetici aynı zamanda İhale Onay Makamı olabileceği gibi bazı durumlarda bir üst kuruluş ya da Kurul da son karardan sorumlu olabilmektedir.

Süreç akışı

Kullanıcı girişi ile temin edilen mevcut süreç akışı Ek-2 Süreç Bilgi Toplama Formu ile verilmiştir. Buna göre mevcut süreç 15 temel adımdan oluşmaktadır:

1) İhale (satın alma) ilanı (İdare)
2) İhale dokümanının teslim alınması (istekliler)
3) Teklif Değerlendirme Heyetinin oluşturulması (İdare)
4) İhale dokümanına ilişkin soruların yöneltilmesi (istekliler)
5) Soruların cevaplanması (Teklif Değerlendirme Heyeti)
6) Tekliflerin sunulması (yüklenici adayları)

7) Teklif Ön Değerlendirme (Teklif Değerlendirme Heyeti)
8) Tekliflerin değerlendirilmesi (Teklif Değerlendirme Heyeti)
9) Teklif Değerlendirme Sonuç Raporunun hazırlanması (Teklif Değerlendirme Heyeti)
10) En İyi ve En Son Tekliflerin alınması (yüklenici adayları – Teklif Değerlendirme Heyeti)
11) Teklif Değerlendirme Sonuç Raporunun revize edilmesi (Teklif Değerlendirme Heyeti)
12) Fiyat yenileme (nihai) (yüklenici adayları – Teklif Değerlendirme Heyeti)
13) Teklif Değerlendirme Sonuç Raporunun revize edilmesi (Teklif Değerlendirme Heyeti)
14) Teklif Değerlendirme Sonuç Raporunun onaylanması (Üst Yönetici)
15) Sonuçların bildirilmesi (İdare)

Yeni süreç akışı da hemen hemen aynı adımları içermekle birlikte, bazı adımların akıllı sözleşme kullanımı ile sistem tarafından otomatik olarak yürütülebilmesi mümkündür. Süreç adımları temel düzeyde aşağıda maddeler halinde verilmiştir.

İdare, teklif koşullarını, kabul edilebilir teklif ve değerlendirme kriterlerini, gereksinimleri, teknik ve idari diğer tüm gerekli bilgileri içeren ihale dokümanlarını oluşturur. Bu ilk adım uygulama örneği için kapsam dışında tutulmuştur. Süreç ihale duyurusu ile başlamaktadır. Buna göre, uygulama için süreç adımları aşağıdaki biçimdedir:

1) Sistemin tasarımı ve kullanıcıların oluşturularak yetkilendirilmesi: Sistem Yöneticisi (SY_i) tanımlanmış kullanıcı rollerine ilişkin tanımlamaları yaparak kullanıcı anahtarlarını oluşturur ve bunları ilgililerine teslim eder. Sistemde kullanılacak anahtarlar gizli ve açık anahtar olmak üzere bir anahtar çifti olup kullanıcılar işlemlerini bu anahtarları kullanarak gerçekleştirirler.
2) İhale (satın alma) ilanı (İdare): Hizmet ya da ürün ihtiyacına bağlı olarak ihale kararı alınıp şartname ya da ihale dokümanları hazırlandıktan sonra ilana çıkılmaktadır. Bir ihale dokümanı, ihalenin şart ve koşullarını, kabul edilebilir bir teklif için gerekli bilgileri ve teklif değerlendirme kriterlerini içerecektir. İhale ilanı Proje Birimi Kullanıcısı (PBK_i) tarafından hazırlanıp, İhale Birimi Kullanıcısı ($İBK_i$) tarafından kontrol edilip Üst Yönetici tarafından onaylandıktan sonra Bilgi İşlem Birimince ($Bİ_i$) duyurulmaktadır.
3) İhale dokümanının teslim alınması (istekliler): İlan doğrultusunda teklif vermeyi tasarlayan kuruluşlar ($İ_i$) ihale dokümanını indirebilecektir. Bu indirme işlemi için ilgili kuruluşun ilanda sayılan şartları taşıyor olması gerekmektedir. Normal süreçte bu şartların kontrolü ihale dokümanının teslimi aşamasında, ihale birimince yapılmakta

olup yeni süreçte dokümanı temin etmek isteyen kuruluşlara İdare tarafından oluşturulmuş bir anahtar verilmekte, kuruluş da bu anahtar ile doküman indirmeyi gerçekleştirmektedir. Önceki süreçte ihale dokümanı tesliminde istenenler yeni tasarımda kullanıcı anahtarının tesliminde istenmektedir. Kullanıcı anahtarının teslim edilebilmesi için gerekli şartların taşındığına dair kontrol ve onay Belge Kontrol ve Teslim Görevlisi ($BKTG_i$) tarafından ya da sisteme dâhil edilecek bir akıllı sözleşme ile gerçekleştirilmektedir. Bu onayı takiben uygun isteklilere kullanıcı anahtarları SY_i tarafından verilmektedir.

4) Teklif Değerlendirme Heyetinin oluşturulması (İdare): Proje Yöneticisi (PY) tarafından teklifleri değerlendirmek üzere bir heyet oluşturulmaktadır. PY tarafından oluşturularak Üst Yönetici (ÜY) tarafından onaylanan heyet listesi (başkan ve üyeler) doğrultusunda sistem kaydı ve anahtarların oluşturularak ilgililerine dağıtılması SY_i tarafından gerçekleştirilmektedir.
5) İhale dokümanına ilişkin soruların yöneltilmesi (istekliler): Teslim alınan dokümanlara ilişkin soru olması halinde, ilgili $İ_i$ sorularını sistem üzerinden kendi anahtarını kullanarak gönderecek, bu sorular kabul edilirken tekliflerin sunulma tarihinden önce olması, soruyu gönderen tarafın kayıtlı kullanıcı olması kontrol edilerek bu sorular sadece heyet üyelerinin erişimlerine açık olacaktır.
6) Soruların cevaplanması (Teklif Değerlendirme Heyeti): Teklif Değerlendirme Heyeti Başkanı (TDHB) ve üyleri ($TDHÜ_i$) kendi erişimlerine açık olan soruları uygun biçimde değerlendirip yanıtları tüm isteklilerin erişimine açık olacak biçimde sistem üzerinden iletirler.
7) Tekliflerin sunulması (yüklenici adayları): İlanda belirtilen sürenin sona ermesinden önce, Adaylar (A_i) tekliflerini sistem üzerinden, kendilerine ait anahtarı kullanarak gönderirler. Gönderilen tekliflerin ihale ilanı ve ihale dokümanlarına uygunluğu onaylanmadan teklifler teslim alınmış sayılmaz. Uygunluk değerlendirmesinin ilk aşamasında teklif dosyasının ve varsa eklerinin mevcudiyet kontrolü sistemce otomatik olarak, akıllı sözleşmeler kullanılarak gerçekleştirilebilir.
8) Teklif Ön Değerlendirme (Teklif Değerlendirme Heyeti): Teklifler, tekliflerin kabul edilebilmesi için gerekli şartların taşındığına dair karar vermek üzere ön değerlendirmeye tabi tutulur. Burada, idari ve teknik olarak vazgeçilmez olan şartların karşılanıp karşılanmadığına bakılır. Burada, geçici teminat mektubu, yetki belgesi gibi mevzuat gereği zorunlu olan belgeler ile teknik olarak özellikle vazgeçilmez olduğu belirtilmiş olan konuların ön kontrolü gerçekleştirilir. Ön değerlendirme sonucunun

olumsuz olması halinde teklif değerlendirme dışı bırakılarak ilgili A_i'nin anahtarları ve erişim izinleri iptal edilir.

9) Tekliflerin değerlendirilmesi (Teklif Değerlendirme Heyeti): Alınan teklifler sadece heyet üyelerinin (TDHB ve $TDHÜ_i$) erişimine açıktır ve hiçbir aday teklif veren diğer adaylar hakkında bilgi sahibi değildir. Değerlendirme aşamasında tekliflere erişim sadece TDHB ve her bir $TDHÜ_i$ tarafından sağlanabilmektedir.
10) Teklif Değerlendirme Sonuç Raporunun hazırlanması (Teklif Değerlendirme Heyeti): İlk değerlendirme sonuçları $TDHÜ_i$ tarafından ilk değerlendirme sonuçları her bir üyenin kendi anahtarı ile TDHB'ye gönderilir. TDHB bu değerlendirmelere dayanarak sonuç raporunu hazırlar ve değerlendime ve onay için PY ve ÜY'ye kendi anahtarı ile gönderir.
11) En İyi ve En Son Tekliflerin alınması (yüklenici adayları – Teklif Değerlendirme Heyeti): İlk değerlendirmeden sonra tüm A_i'dan tekliflerinin fiyat kısımlarının daha önce verilmiş olan teklifi aşmamak kaydıyla, belirli bir süre içerisinde revize edilmesi istenir. Bu talep PY tarafından, kendi anahtarı ile gerçekleştirilir. İlk tekliflerin sunulmasına benzer biçimde tüm A_i'ler tarafından yeni fiyat teklifleri sunulur. Sunulan bu tekliflerin uygunluk kontrolleri akıllı sözleşme ile gerçekleştirilir. Belirtilen sürenin bitişinden itibaren sunulan teklifler kabul edilmez.
12) Teklif Değerlendirme Sonuç Raporunun revize edilmesi (Teklif Değerlendirme Heyeti): Alınan yeni tekliflere göre $TDHÜ_i$ tarafından tekrar değerlendirme yapılarak Teklif Değerlendirme Sonuç Raporuna bu değerlendirme sonuçları eklenmek üzere TDHB'ye iletilir. TDHB bu değerlendirmelere dayanarak sonuç raporunu revize eder ve değerlendime ve onay için PY ve ÜY'ye kendi anahtarı ile gönderir.
13) Fiyat yenileme (nihai) (yüklenici adayları – Teklif Değerlendirme Heyeti): ÜY tarafından nihai olarak teklif fiyatlarının yenilenmesi istenebilir. Bu durumda, ÜY anahtarı ile A_i'den tekliflerini belirli bir süre içerisinde nihai olarak yenilemeleri istenir. İlk tekliflerin sunulmasına benzer biçimde tüm A_i'ler tarafından yeni fiyat teklifleri sunulur. Sunulan bu tekliflerin uygunluk kontrolleri akıllı sözleşme ile gerçekleştirilir. Belirtilen sürenin bitişinden itibaren sunulan teklifler kabul edilmez.
14) Teklif Değerlendirme Sonuç Raporunun revize edilmesi (Teklif Değerlendirme Heyeti): Alınan nihai teklif fiyatlarına göre TDHB tarafından Teklif Değerlendirme Sonuç Raporu güncellenir ve değerlendime ve onay için PY ve ÜY'ye kendi anahtarı ile gönderir.

15) Teklif Değerlendirme Sonuç Raporunun onaylanması (Üst Yönetici): Uygun görüşle sunulan Teklif Değerlendirme Raporu ÜY tarafından onaylanarak değerlendirme sonucuna karar verilir.
16) Sonuçların bildirilmesi (İdare): ÜY tarafından onaylanan değerlendirme sonucuna göre Yüklenici (Y) olarak belirlenen A_i tüm A_i'lere bildirilir.

Temel hedefler ve kurallar

Sürecin blokzincir ile tasarımında dikkate alınacak temel hedefler aşağıdaki biçimdedir:

1) İdare, ihale duyurusunu yayınladıktan sonra ihale dokümanlarını değiştiremez. Teklifler alınmadan önce değişiklik gerektiren bir durum olması halinde yeniden ilan yayınlanır. Değişikliğe izin verilmemesinin temel amacı ihale şartlarının teklif verecek kuruluşlar lehine değiştirilmesinin önlenmesidir.
2) İhale dokümanını temin etmek için belirli şartların taşınması gerekmektedir. Bunlar ihale dokümanı için gerekli ücretin ödenmesi, ihale dokümanlarının gizliliği ve güvenliğinin sağlanacağına dair taahhüt verilmesi ve ihaleye teklif verecek firma tarafından resmi olarak yetkilendirildiğine dair kanıt biçimindedir.
3) Hiçbir yüklenici adayının teklif veren diğer adaylar hakkında bilgi sahibi olmaması gerekmektedir.
4) İhale için teklif verme süresi dolduktan sonra hiçbir şekilde teklif sunulamaz.
5) İhale için teklif verme süresi sona erdikten sonra tekliflere yalnızca Teklif Değerlendirme Heyetince erişilebilir.
6) Teklif vermek için belirlenen süre bitmeden önce Teklif Değerlendirme Heyeti Üyeleri ya da Sistem Yöneticisi de dâhil olmak üzere hiçbir taraf tekliflere erişim sağlayamaz. Bu, teklif veren tarafından üretilmiş olan anahtarın ancak tüm tekliflerin açılması için karar alındıktan sonra kullanıma açılması ile sağlanır.
7) Teklifler bir kez sunulduktan sonra ne teklifi sunan, ne değerlendiren ne de sistemi yöneten taraflarca değiştirilemez.
8) İstekliler sadece bir kez teklif verebilir.
9) Değerlendirme sonucunun ilanına kadar rolleri tanımlı kullanıcılar dışında sürece kimse dâhil olamamaktadır. Ancak; İdarenin isteği ve mevzuatın izin vermesi halinde vatandaşlar süreci hazırlanacak bir portal üzerinden takip edebilir.

Akıllı sözleşmenin kullanımı

1) Tekliflerin teslim alınması aşamasında istekliler İdareden işlemleri gerçekleştirmek için anahtar talebinde bulunur. İdare tarafından üretilecek olan anahtarların teslimi için temelde üç şart bulunmaktadır: teklifi verecek olan firmanın doğrudan başvuru yapması ya da yetkilendirdiği bir temsilci tarafından ihale dokümanları temin edilecekse yetki belgesi, teklifi alacak olan firmanın yetkili çalışanına ilişkin yetki belgesi, doküman bedelinin yatırıldığına dair ödeme kanıtı. Akıllı sözleşme ile bu sayılarınların doğrulanması halinde ihale dokümanları isteklilerin erişimine açılacaktır.
2) Sunulan teklif, isteklilerin imza anahtarı ile imzalanır ve akıllı sözleşmelere aktarılır. Bu İmza anahtarının yetkili teklif veren şirket olup olmadığı doğrulanır.
3) İhale ilanında belirtilen doküman teslim alma süresi sona erdiğinde akıllı sözleşme dokümana erişimi sonlandıracaktır.
4) İhale ilanında belirtilen tekliflerin sunum süresi sona erdiğinde akıllı sözleşme tekliflerin kabul edilmesini durduracaktır.
5) İhale ilanında belirtilen tekliflerin sunulma süresi geçmeden, sunulmuş olan tekliflere erişim engellenecektir.
6) Teknik kısımlara ilişkin değerlendirmeler tamamlanmadan Teklif Değerlendirme Heyeti üyelerinin teklif fiyatlarına erişimleri engellenecektir.

Süreç işlem hacmi (maksimum ve beklenen)

Detayları Ek-2 Süreç Bilgi Toplama Formunun ikinci maddesinde verilmiş olan Kamu İhale Kurumu'nun 2011 – 2021 yılları arası Kamu Alımları İzleme Raporlarından alınan ihale sayılarına göre İdare başına düşen ihale sayısı yılda ortalama 12,4'tür. Belirtilen dönemde her yıl için toplam ihale sayısının toplam İdare sayısına bölümü ile bulunan ortalama değer en fazla 14, en az 10 olarak gerçekleşmiştir. Bu da seçilen örnek uygulama için işlem hacminin herhangi bir finansal süreç ile kıyaslanamayacak düzeyde düşük olduğunu, işlem hacminin blokzincir tasarımı için önemli bir kısıt oluşturmadığını göstermektedir.

Süreç işlem hızı

Ek-2 Süreç Bilgi Toplama Formunun dördüncü maddesinde de yer verildiği üzere, süreç işlem hızına ilişkin bir veri temin edilememiş olmakla birlikte ihalenin kapsamı, istekli ve

yüklenici adayı sayısı, işin aciliyeti gibi nedenlerle ihalelerin işlem hızı değişkenlik göstermektedir. İşlem hızı seçilen uygulama için ihale ilanının yayınlanması ile teklif değerlendirme sonucunun duyurulması arasında geçen süredir. İşlem hacmine benzer biçimde, işlem hızı da herhangi bir finansal süreç ile kıyaslanamayacak düzeyde düşük olup uygulama için seçilen sürecin hâlihazırdaki tamamlanma zamanının blokzincir ile tasarlanan sistem ve akıllı sözleşme kullanımı ile kayda değer ölçüde kısaltılabileceği değerlendirilmektedir.

Veri içeriği ve sınıflandırma (blok yapısı)

Ek-2 Süreç Bilgi Toplama Formunun altıncı maddesinde de yer verildiği üzere blok içerisinde tutulacak veri, bloğu tanımlayan metaveri ve işlemleri içeren veriler olmak üzere iki tiptir. Bloğun içerisinde yer alacak veriye karar verilirken süreç içerisinde kullanılan veriler dikkate alınarak bir tasarım yapılmalıdır. Bitcoin gibi finansal amaçlı blokzincirlerde blok sadece metaveri yanında transfer işlemlerini içerdiğinden bloğun tasarımı standart ve nispeten kolaydır. Ancak, içerisinde fazla sayıda ve çeşitte veri içeren bir blokzincir sisteminde blok yapısı biraz daha karmaşık bir hâl almaktadır. Hatırlanacağı üzere, blokzincir teknolojisinin getirdiği yenilikler ve sunduğu avantajlar bu blok yapısından kaynaklanmaktadır. Bu nedenle, uygulama konusu olan kamu ihale süreci için de benzer bir biçimde, içerisinde özdeş veri grupları bulunan ve art arda gelen bir blok yapısı tasarlanmalıdır.

Bu tasarım için ilk akla gelen alternatif her bir blok bir yüklenici adayını temsil etmek üzere, blok içerisine ihale dokümanına ilişkin tüm cevaplar ilave edilerek tekliflerin sunulma sırasına göre bloklar art arda eklenerek bir zincir oluşturulmasıdır. Ancak bu durumda her bir ihale için bir blokzincir oluşturulacak, yüklenici adayı sayısı kadar blok eklendikten sonra sistem kullanılamayacaktır. Bu nedenle bu tasarım uygun bulunmamıştır.

İhale konusundan bağımsız bir biçimde blokzinciri sürekli büyüyen bir kayıt defteri biçiminde yaratacak jenerik blok yapısını oluşturabilmek için tasarlanan sistem aşağıdaki özellikleri taşıyacaktır:

1) Sistemdeki her bir kullanıcının kendisine ait bir adresi bulunacaktır.

2) İhale dokümanları ve bu dokümanlara verilen cevaplar ile kanıtlayıcı belgeler blokzincirde tutulmayacak, zincir dışında (off-chain) tutulacak bu bilgi ve belgelerin hash değerleri kullanılacaktır.
3) Sistemde yer alacak tüm bilgi ve belgelerin hash değerleri ile işlem yapılacaktır.
4) Bu hash değerleri ile işlemleri gerçekleştirmek için süreç içerisinde kullanılacak bilgi ve belgeler gruplandırılarak yönetilecektir. Bu gruplandırma aşağıdaki biçimde olacaktır:
   a. İdari şartname
   b. Teknik şartname
   c. Taslak sözleşme
   d. İdareye sorulan sorular
   e. Yüklenici adaylarına verilen cevaplar
   f. Yüklenici adaylarına sorulan sorular
   g. İdareye verilen cevaplar
   h. Süreç içerisindeki dokümanlar
      i. Geçici Teminat Mektubu
      ii. Yetki Belgesi
      iii. Teklif Mektubu
      iv. Teklif Değerlendirme Sonuç Raporu
5) Dördüncü maddede sayılmış olan tüm bilgi ve belgeler hazırlayan tarafça hash değeri alındıktan sonra ilgilisine gönderilecek, bu gönderme işlemi gönderici adresi, alıcı adresi, zaman damgası, mesaj başlığı (hangi veri sınıfına ait olduğu) bilgilerini içerecektir.
6) İşlem talepleri öncelikle bir havuzda toplanacak, daha sonra her bir işlem mesaj başlığı kontrol edilerek aynı mesaj başlığına sahip işlemlerden bir blok yaratılacaktır.
7) Oluşturulan bloklar birbirlerine blok hash değeri ile bağlanacaktır.
8) Zincir dışında tutulan bilgi ve belgeler değerlendirilirken sistem tarafından yeniden hash değeri alınacak, blokzincirde tutulan hash değerleri ile karşılaştırıldıktan sonra değerlendirme işlemine geçilecektir.
9) Sistem tasarımında “Temel hedefler ve kurallar” alt başlığında sayılmış olan şartlar dikkate alınacak, adres sahiplerinin blok verilerine ve zincir dışında tutulan verilere erişimleri kontrollü bir biçimde gerçekleştirilecektir.

Buna göre, blokzinciri oluşturan blokların yapısı Çizelge 5.56’da verilmiştir:

Çizelge 5.56. Kamu İhale Süreci blokzincir blok yapısı

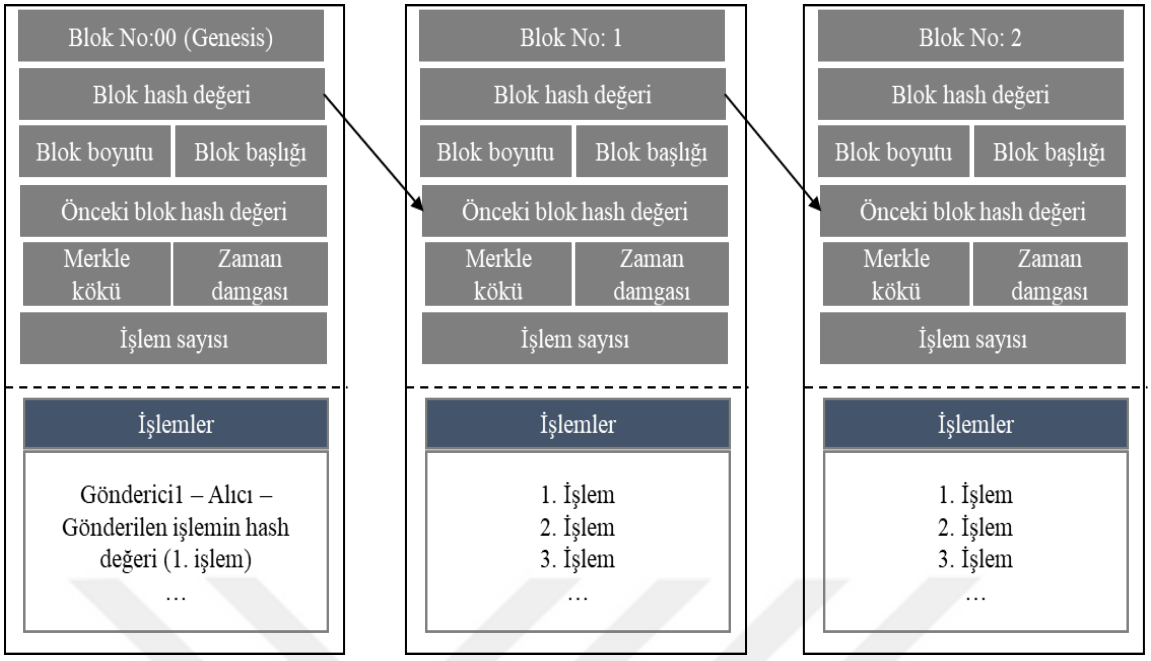
	Veri	Açıklama	
Blok bilgileri	Blok #	Blok numarası (ardışık olarak devam eden, benzersiz blok no)	
	Blok Boyutu	Bu alanı takip eden bloğun boyutu	
	Blok başlığı	Bloğun hash değeri, takip eden blokta kullanılacak olan	
	Blok Konu Başlığı	Blok içerisinde yer alan işlemlerin sınıfı: • İhale şartları (00) • İdari şartname (01) • Teknik şartname (02) • Taslak sözleşme (03) • İdareye sorulan sorular (04) • İsteklilere verilen cevaplar (05) • Geçici Teminat Mektubu (06) • Yetki Belgesi (07) • Teklif Mektubu (08) • Teklifler-İdari (09) • Teklifler-Teknik (10) • Teklifler-Taslak Sözleşme (11) • Yüklenici adaylarına sorulan sorular (12) • İdareye verilen cevaplar (13) • Teklif Değerlendirme Sonuç Raporu (14) • Yüklenici Seçim Kararı (15)	
	Önceki bloğun hash değeri	Zincirdeki önceki bloğun (parent) hash referansı	
	Merkle Ağacı Kökü	Bu bloktaki işlemlerin Merkle ağacının kökünün (hash) değeri	
	Zaman damgası	Bloğun yaklaşık yaratılma zamanı (Unix Epoch saniye)	
	İşlem sayısı	Bloğun içerdiği işlemlerin adedi	
Kullanıcı bilgileri[11]	İstekli(ler)	$İ_i$	Her bir aday için Sistem Yöneticisi tarafından ya da otomatik olarak bir adres oluşturulacak, bu adres şartları taşıyan adaylara ihale dokümanlarını iletmek için kullanılacaktır. İstekliler, teklif sunmaları halinde bu adresi kullanmaya devam edeceklerdir.
	Aday(lar)	A_i	Adayların tamamı İstekliler arasında yer almak zorundadır. Yani; Adaylar için ayrı bir adres tanımlaması yapılmayacak, $İ_i$ için belirlenmiş olan adresler kullanılmaya devam edilcektir. Bu adres aynen mevcut kriptopara sisteminde olduğu gibi sahibi tarafından işlem gerçekleşirmek için (teklif sunma, soru sorma, cevap verme vb.) kullanılacaktır.
	Yüklenici	Y	Değerlendirme sonucunda, diğerleri arasında teklifi en uygun bulunan Adaydır. Yeni bir adres tanımlanmayacaktır. Yüklenici Seçim Kararının iletileceği kullanıcıdır.
	Proje Birimi kullanıcısı	PBK_i	İhale ilanının hazırlanarak onaya sunulması işlemini gerçekleştiren bu kullanıcının tasarlanan sistemdeki rolü Teklif Değerlendirme Heyeti oluşturulmadan önceki ihale işlemlerini yürütmektir.
	Belge kontrol ve teslim görevlisi	$BKTG_i$	İhale şartlarının taşınıp taşınmadığı kontrolünü gerçekleştirecek kullanıcıdır. Bu kullanıcı rolü blokzincir sisteminde otomatik olarak gerçekleştirilebilecektir. Ancak, blokzincirde ilgili şartlara ilişkin sadece hash değeri tutulacağından, zincir dışı (off-chain) bilgi ve belgelerin kontrolünün yapılması gerekebilecektir. Kontrolden sonra, uygun isteklilere ihale dokümanlarının gönderilmesinden sorumludur. Uygun adaylara ilgili dokümanların hash değerlerini ilgili blok sınıfı altında göndermek, aynı zamanda zincir dışı sistemde dokümanları teslim etmekten sorumludur.
	Sistem Yöneticisi	SY_i	Sistem yöneticisinin bloklar içerisindeki işlemlere ilişkin doğrudan bir rolü bulunmamakla birlikte, blok içerisinde işlem gerçekleştirmesi halinde kullanılmak üzere diğer kullanıcılarla aynı biçimde bir adresi bulunacaktır. Kullanıcı kayıt işlemlerinin gerçekleştirileceği sistemin otomatik çalışan bir arayüz olması uygun değerlendirilmekte olup Sistem Yöneticisi bu arayüzün yönetiminden ve bakımından sorumludur.

[11] "Süreçte rol alan taraflar ve rolleri" alt başlığında verilmiş olan kullanıcılar

	Veri	Açıklama	
	Bilgi İşlem Kullanıcısı	$Bİ_i$	Bloklar içerisinde yer alan işlemlere ilişkin doğrudan bir rolü bulunmamakla birlikte, blok içerisinde işlem gerçekleştirmesi halinde kullanılmak üzere diğer kullanıcılarla aynı biçimde bir adresi bulunacaktır.
	İhale Birimi Kullanıcısı	$İBK_i$	Bloklar içerisinde yer alan işlemlere ilişkin doğrudan bir rolü bulunmamakla birlikte, blok içerisinde işlem gerçekleştirmesi halinde kullanılmak üzere diğer kullanıcılarla aynı biçimde bir adresi bulunacaktır. Bu kullanıcıya en son aşamada, Yüklenici Seçim Kararı iletilecektir.
	Teklif Değerlendirme Heyeti başkanı	TDHB	Teklif Değerlendirme Heyeti ile Proje Yöneticisi arasında iletişi sağlayan kullanıcıdır. Bu kullanıcı adresi ile sadece Proje Yöneticisi arasında işlem gerçekleştirilebilmektedir.
	Teklif Değerlendirme Heyeti üyeleri	$TDHÜ_i$	Her bir heyet üyesi için ayrı bir adres oluşturulacak, heyet üyeleri işlemlerini bu adresleri kullanarak gerçekleştirecektir.
	Proje Yöneticisi	PY	Değerlendirme sürecinde hem Üst Yönetici hem de Yüklenici Adayları ile Heyet arasındaki işlemleri kontrol ederek onaylayan ve yönlendiren kullanıcı olup yetkisi dâhilindeki tüm işlemleri adresi ile gerçekleştirecektir.
	Üst Yönetici	ÜY	Yüklenici Seçim Kararını onaylayan, süreç içerisinde diğer kullanıcıların yetkisi bulunmayan konularda karar veren kullanıcı rolüdür.
İşlem Bilgileri	İdari Şartlar	İlgili dokümanın hash değerini ifade etmektedir. İdare kullanıcısından gönderildiğinde ihale dokümanının ilan edilen halinin, yüklenici adayından gönderildiğinde ise verilen cevapların ve tekliflerin hash değeridir. Zincir dışında orijinalleri iletilen dokümanların hash değeleri alınıp blok içerisindeki hash değeri ile karşılaştırılarak orijinallik kontrolü yapılır.	
	Teknik Şartlar		
	Taslak sözleşme		
	İdareye sorulan sorular		
	Yüklenici adaylarına verilen cevaplar		
	Yüklenici adaylarına sorulan sorular		
	İdareye verilen cevaplar		
	Geçici Teminat Mektubu		
	Yetki Belgesi		
	Teklif Mektubu		
	Teklif Değerlendirme Sonuç Raporu		
	Yüklenici Seçim Kararı		

Her blok temelde iki alandan oluşmaktadır: blok bilgileri ve işlem bilgileri. İşlem bilgileri kullanıcı bilgilerini de içerdiğinden Çizelge 5.56'da kullanıcılar ayrı bir alan olarak gösterilmiş olmasına karşın blok yapısında kullanıcı tanımlamasına yönelik bir alan bulunmamaktadır. Her bir blokta birden fazla işlem yer alabilecek olup işlem sayısı blok için öngörülecek maksimum boyutla sınırlıdır. Yani; Bitcoin örneğinde olduğu gibi, bir blok için maksimum boyut 1 MB belirlenecek olursa, her bir blok yaklaşık 2 000 işlemi içerebilecektir. Ancak, uygulama örneğinde gerçekleştirilecek işlemler herhangi bir ödeme sistemindeki işlem hacminin çok altında olduğundan blok boyutu önemli bir kısıt oluşturmamaktadır.

Uygulama örneğindeki blok yapısı daha önceki bölümlerde yer verilmiş olan blok yapılarına benzer ve Çizelge 5.56'da verilmiş olan alanları içerecek biçimde Şekil 5.3'te verilmiştir.



Şekil 5.3. Kamu İhale Süreci blokzincir uygulaması örnek blok yapısı

Çizelge 5.56'da verilen yapı ve Kamu İhale Sürecinin adımları dikkate alınarak tasarlanan sistem için önerilen blok yapısı 5 istekli ($İ_i$) ve 4 yüklenici adayı (A_i) için örnek içerikle birlikte aşağıdaki biçimdedir:

1) Sistem kullanıcıları için gizli ve açık anahtarların oluşturulması: Sistem içerisinde, kullanıcıların kimliklerini ispatlamaları, kimliklerin doğrulanması ve kullanıcılar arasında işlemlerin gerçekleştirilmesi için anahtar çiftleri kullanılmaktadır. Açık Anahtar Altyapısı (PKI) adı verilen gizli ve açık anahtar yapısı bu rolü itibarıyle sistemin en vazgeçilmez unsurlarından biridir. Anahtarların üretilmesi genellikle Sertifika Otoriteleri (CA - Certificate Authorities) tarafından sunulan bir hizmettir. Önerilen yapıda, Hyperledger Fabric platformunun Üyelik Hizmeti Sağlayıcısı (MSP - Membership Service Provider) adı verilen aracı ile bu anahtarların yönetimi gerçekleştirilmektedir. Buna göre, bir Sertifika Otoritesi vasıtasıyla üretilen ve önerilen blokzincir platformu ile yönetilen anahtarlara ilişkin örnekler Çizelge 5.57'de sunulmuştur. Bu örnekte sunulan anahtarlar en eski asimetrik kriptografik algoritmalardan biri olan RSA (Rivest–Shamir–Adleman) ile üretilmiş olan 512 bitlik anahtar çiftleridir. Her bir kullanıcı için bu biçimde bir anahtar çifti üretilerek kullanılacaktır.

Çizelge 5.57. Sistem kullanıcıları için üretilen anahtar yapısı örneği

Kull.	**Açık (public) anahtar**	**Gizli (private) anahtar**
A_1	MFswDQYJKoZIhvcNAQEBBQADSgAwRwJAax Pa0C7G3imL9FjfTy8Wrw9C7CfKb6qp A33J3DkefSo78dLXXSJxEjoAP6Lnha6CL0GBy4 Y/sHOnWVvJUBKwwQIDAQAB	MIIBOgIBAAJAaxPa0C7G3imL9FjfTy8Wrw9C7Cf Kb6qpA33J3DkefSo78dLXXSJx EjoAP6Lnha6CL0GBy4Y/sHOnWVvJUBKwwQID AQABAkBNTPgacqp+l9/Bdqc/su7d UlctxUwPcVSygIzJvzKTiIn+V2gI41EQ7jPSUdYzT JS3efa66j+ed+liZ18yVJxB AiEAs+GyRJg+CZMc1iAShDwZydQ5qnYoKew54 IJx05CaOesCIQCYY2dxb7py0JWQ Ry80mJuwdJPBOwstLlMv4oLBO0BJAwIhAJWcJh T/Ornj7Zv6WOw6wIgpRz0LwSP9 IbYlSF7aaiu5AiBOi84h1ikQTRsKRua6AX8eMLiH/ NsB6sLOB77Fwrib6QIhAKuo OgQGkoZM1TfHVXVbjOdJW//HfD4IiRWnqejBOd 0i
A_2	MFswDQYJKoZIhvcNAQEBBQADSgAwRwJAeh 5+0jtkZeJc+kA6EYdFr/aKl0+15+2/ 7cSOE8GIsBntOMyuzns0r2BRTnZUMK8w4R4VrG/Or1cnWOW265EyAQIDAQAB	MIIBOQIBAAJAeh5+0jtkZeJc+kA6EYdFr/aKl0+15 +2/7cSOE8GIsBntOMyuzns0 r2BRTnZUMK8w4R4VrG/Or1cnWOW265EyAQID AQABAkAHOeK7QfRw6vIhhMdq3hxL i0UsKvVSogjnYugdVyhlcy2n8BKikZbJ9SlEvUqnS ReXhLP1ozcVVLhDpE87BjIZ AiEA5Y4I8/6KlxwDZiRtDonDq6E+c5xhuJ8N+Dfe u7fRfPcCIQCIL/9eOBgiSuIv S+4dWINLHg4kFi7H/+1zwlN/zRHixwIgFDpa4Z1J ex1V01dcYM6U9nfD+A4MsmcZ pQjPUL1W8WsCIG4aqBKLtW9cLXvhnpSZMCT2 GqawTIgj8N0rGgj0SeaXAiEAxg/m iGYbsL892elrCZ3ZdXk6vrhTuBmHgRnQatr8FP0=
$Bİ_1$	…	…
…	…	…

Çizelge 5.57'de örneği verilmiş olan açık anahtarlar kullanıcıların adresi, gizli anahtarlar ise imzası işlevini görmekte olup her bir işlemin göndericisi ve alıcısı bu açık anahtarlar ile gerçekleştirilcek ve izlenecek, kullanıcıların kimlikleri ise gizli anahtarlarla doğrulanacaktır.

Anahtarların temin edilebilmesi için ihale duyurusunun yapılmış olması, isteklilerin ihale dokümanı için öngörülen ücreti yatırmış olmaları, teklif vermeye yetkili olduklarını kanıtlamaları ve anahtar sahibinin yetkilendirilmiş olması şartları sağlanmalıdır.

Sürecin sonraki adımlarındaki işlemlere ilişkin örneklerde kullanıcı adresleri için Pub(Kullanıcı) notasyonu kullanımıştır.

2) İhale şartları blok yapısı: İhale ilanı tüm isteklilerin erişim sağlayabileceği bir doküman olup içerisinde ihale katılım şartları, ihale dokümanlarının alınması için öngörülen süre gibi bilgileri içermektedir. Örnek uygulamada ihale ilanının onaylı bir tedarikçi listesine ya da önceden belirlenmiş olan uygun adaylara, davet usulü ile gönderileceği

varsayılmıştır. Buna göre, davet edilecek firmalar listesinde yer alan tüm adaylar sisteme kaydolarak anahtarlarını temin ettikten sonra ilk blok (genesis) yaratılmakta ve bu blok ilgili ihale davet dosyasının hash değerinin gönderildiği işlemleri içermektedir. Tasarıma bağlı olarak, bloğa erişimin tüm kullanıcılara açılması halinde kendisine ilan gönderilen kuruluşlar kaç adaya ilan gönderildiğini görebilecek, ancak bunların kimler olduklarını tespit edemeyeceklerdir. Buna göre, sistemin ilk bloğunun içerdiği bilgiler Çizelge 5.58'de verilen örnekteki gibi olacaktır:

Çizelge 5.58. İhale şartları (00) başlıklı ilk (genesis) blok yapısı

Alan adı	İçerik	Açıklama
Blok bilgileri		
Blok #	0	Genesis blok
Blok başlığı	H_{BLOK0}	Bloğun hash değeri
Blok Boyutu	… byte	Bloğun byte cinsinden boyutu
Blok konu başlığı	00	"İhale şartları" başlığını ifade etmektedir
Önceki bloğun hash değeri	0X	İlk blok olduğu için önceki bloğa ait hash değeri bulunmamaktadır
Merkle kökü	$H^{12}{}_{12345}$	Alt indis olarak verilmiş olan işlemlerin hash değerlerinden elde edilen Merkle kök değerini ifade etmektedir
Zaman damgası	1666274660	Unix Epoch zamanı (Örnek için 20 Ekim 2022 14:04:20 zamanını ifade etmektedir)
İşlem sayısı	5	Bloğun işlemler kısmında yer alan işlem sayısı (5 İstekliye gönderilen ilanı ifade eden 5 işlem listelenmektedir)
İşlemler		
İşlem 1	$Pub(PBK_i) \rightarrow Pub(İ_1) : H_{(ihale\ şartları)}$	Proje Birimi kullanıcısı "ihale ilanı" dokümanının hash değerini birinci İstekliye göndermektedir
İşlem 2	$Pub(PBK_i) \rightarrow Pub(İ_2) : H_{(ihale\ şartları)}$	Proje Birimi kullanıcısı "ihale ilanı" dokümanının hash değerini ikinci İstekliye göndermektedir
İşlem 3	$Pub(PBK_i) \rightarrow Pub(İ_3) : H_{(ihale\ şartları)}$	Proje Birimi kullanıcısı "ihale ilanı" dokümanının hash değerini üçüncü İstekliye göndermektedir
İşlem 4	$Pub(PBK_i) \rightarrow Pub(İ_4) : H_{(ihale\ şartları)}$	Proje Birimi kullanıcısı "ihale ilanı" dokümanının hash değerini dördüncü İstekliye göndermektedir
İşlem 5	$Pub(PBK_i) \rightarrow Pub(İ_5) : H_{(ihale\ şartları)}$	Proje Birimi kullanıcısı "ihale ilanı" dokümanının hash değerini beşinci İstekliye göndermektedir

3) İdari şartname blok yapısı: İhale ilanı gönderildikten sonra, istekliler ilanda yer verilen koşulları karşılamaları halinde teklif sunabilmek için ihale dokümanlarını temin edeceklerdir. Sürecin mevcut işleyişinde, istekliler İdare'ye ihale dokümanı bedelinin yatırıldığına dair dekont, teklif vermeye yetkili olunduğuna dair yetki belgesi ve ihale dokümanını almak üzere ilgili personelin yetkilendirildiğine dair yetki belgesi ile başvurarak dokümanları teslim almaktadır. Önerilen sistemde ise ihale dokümanları teknik, idari ve taslak sözleşme ile süreç içerisindeki dokümanlar olarak alt kısımlara ayrılmış olup bunların her biri ayrı ayrı teslim edilmektedir. Bu kısımlara ayırma işlemi tekliflerin teknik ve idari kısımlarının ayrı ayrı değerlendirilebilmesini sağlamak,

[12] H: hash işlemini göstermektedir

tekliflerin ön değerlendirmesini yaparken sunulması zorunlu olan dokümanların kontrolünü daha kolay biçimde gerçekleştirmek ve blok yapısını özdeş hale getirmek amacıyla yapılmaktadır. Buna göre, sistemin ikinci bloğunun içerdiği bilgiler Çizelge 5.62'de verilen örnekteki gibi olacaktır:

Çizelge 5.59. İdari şartname (01) başlıklı ikinci blok yapısı

Alan adı	İçerik	Açıklama
Blok bilgileri		
Blok #	1	İkinci blok
Blok başlığı	H_{BLOK1}	Bloğun hash değeri
Blok Boyutu	… byte	Bloğun byte cinsinden boyutu
Blok konu başlığı	01	"İdari şartname" başlığını ifade etmektedir
Önceki bloğun hash değeri	H_{BLOK0}	İlk bloğun hash değeri
Merkle kökü	H_{12345}	Alt indis olarak verilmiş olan işlemlerin hash değerlerinden elde edilen Merkle kök değerini ifade etmektedir
Zaman damgası	1667296800	Unix Epoch zamanı (Örnek için 1 Kasım 2022 10:00:00 GMT zamanını ifade etmektedir)
İşlem sayısı	5	Bloğun işlemler kısmında yer alan işlem sayısı (5 İstekliye gönderilen idari şartname hash değerini ifade eden 5 işlem listelenmektedir)
İşlemler		
İşlem 1	$Pub(BKTG_i) \rightarrow Pub(İ_1) : H_{(idari\ şartname)}$	Proje Birimi kullanıcısı "idari şartname" dokümanının hash değerini birinci İstekliye göndermektedir
İşlem 2	$Pub(BKTG_i) \rightarrow Pub(İ_2) : H_{(idari\ şartname)}$	Proje Birimi kullanıcısı "idari şartname" dokümanının hash değerini ikinci İstekliye göndermektedir
İşlem 3	$Pub(BKTG_i) \rightarrow Pub(İ_3) : H_{(idari\ şartname)}$	Proje Birimi kullanıcısı "idari şartname" dokümanının hash değerini üçüncü İstekliye göndermektedir
İşlem 4	$Pub(BKTG_i) \rightarrow Pub(İ_4) : H_{(idari\ şartname)}$	Proje Birimi kullanıcısı "idari şartname" dokümanının hash değerini dördüncü İstekliye göndermektedir
İşlem 5	$Pub(BKTG_i) \rightarrow Pub(İ_5) : H_{(idari\ şartname)}$	Proje Birimi kullanıcısı "idari şartname" dokümanının hash değerini beşinci İstekliye göndermektedir

4) Teknik Şartname blok yapısı: İdari şartname blok yapısı ile aynı biçimde, her bir İstekliye teslim edilen teknik şartname hash değerlerinin blokzincirde kaydedildiği bloktur. Bu bloğun yapısı Çizelge 5.60'ta verilmiştir.

Çizelge 5.60. Teknik şartname (02) başlıklı üçüncü bloğun yapısı

Alan adı	İçerik	Açıklama
Blok bilgileri		
Blok #	2	Üçüncü blok
Blok başlığı	H_{BLOK2}	Bloğun hash değeri
Blok Boyutu	… byte	Bloğun byte cinsinden boyutu
Blok konu başlığı	02	"Teknik şartname" başlığını ifade etmektedir
Önceki bloğun hash değeri	H_{BLOK1}	Önceki bloğun hash değeri
Merkle kökü	H_{12345}	Alt indis olarak verilmiş olan işlemlerin hash değerlerinden elde edilen Merkle kök değerini ifade etmektedir
Zaman damgası	1667296800	Unix Epoch zamanı (Örnek için 1 Kasım 2022 10:00:00 GMT zamanını ifade etmektedir)
İşlem sayısı	5	Bloğun işlemler kısmında yer alan işlem sayısı (5 İstekliye gönderilen teknik şartname hash değerini ifade eden 5 işlem listelenmektedir)

İşlemler		
İşlem 1	$Pub(BKTG_i) \rightarrow Pub(İ_1):H_{(teknik\ şartname)}$	Proje Birimi kullanıcısı "teknik şartname"nin hash değerini birinci İstekliye göndermektedir
İşlem 2	$Pub(BKTG_i) \rightarrow Pub(İ_1):H_{(teknik\ şartname)}$	Proje Birimi kullanıcısı "teknik şartname"nin hash değerini ikinci İstekliye göndermektedir
İşlem 3	$Pub(BKTG_i) \rightarrow Pub(İ_1):H_{(teknik\ şartname)}$	Proje Birimi kullanıcısı "teknik şartname"nin hash değerini üçüncü İstekliye göndermektedir
İşlem 4	$Pub(BKTG_i) \rightarrow Pub(İ_1):H_{(teknik\ şartname)}$	Proje Birimi kullanıcısı "teknik şartname"nin hash değerini dördüncü İstekliye göndermektedir
İşlem 5	$Pub(BKTG_i) \rightarrow Pub(İ_1):H_{(teknik\ şartname)}$	Proje Birimi kullanıcısı "teknik şartname"nin hash değerini beşinci İstekliye göndermektedir

5) Taslak sözleşme blok yapısı: Birinci ve ikinci blok yapısına benzer biçimde, yüklenici adaylarından okunduğu ve kabul edildiğine dair kabul ve onay istenen hükümler içeren taslak sözleşmenin her bir İstekliye teslim edilen hash değerinin blokzincire kaydedildiği bloktur. Bu bloğun yapısı Çizelge 5.61'te verilmiştir.

Çizelge 5.61. Taslak sözleşme (03) başlıklı dördüncü bloğun yapısı

Alan adı	İçerik	Açıklama
Blok bilgileri		
Blok #	3	Dördüncü blok
Blok başlığı	H_{BLOK3}	Bloğun hash değeri
Blok Boyutu	… byte	Bloğun byte cinsinden boyutu
Blok konu başlığı	03	"Taslak sözleşme" başlığını ifade etmektedir
Önceki bloğun hash değeri	H_{BLOK2}	Önceki bloğun hash değeri
Merkle kökü	H_{12345}	Alt indis olarak verilmiş olan işlemlerin hash değerlerinden elde edilen Merkle kök değerini ifade etmektedir
Zaman damgası	1667296800	Unix Epoch zamanı (Örnek için 1 Kasım 2022 10:00:00 GMT zamanını ifade etmektedir)
İşlem sayısı	5	Bloğun işlemler kısmında yer alan işlem sayısı (5 İstekliye gönderilen taslak sözleşme hash değerini ifade eden 5 işlem listelenmektedir)
İşlemler		
İşlem 1	$Pub(BKTG_i) \rightarrow Pub(İ_1):H_{(taslak\ sözleşme)}$	Proje Birimi kullanıcısı "taslak sözleşme"nin hash değerini birinci İstekliye göndermektedir
İşlem 2	$Pub(BKTG_i) \rightarrow Pub(İ_1): H_{(taslak\ sözleşme)}$	Proje Birimi kullanıcısı "taslak sözleşme"nin hash değerini ikinci İstekliye göndermektedir
İşlem 3	$Pub(BKTG_i) \rightarrow Pub(İ_1): H_{(taslak\ sözleşme)}$	Proje Birimi kullanıcısı "taslak sözleşme"nin hash değerini üçüncü İstekliye göndermektedir
İşlem 4	$Pub(BKTG_i) \rightarrow Pub(İ_1): H_{(taslak\ sözleşme)}$	Proje Birimi kullanıcısı "taslak sözleşme"nin hash değerini dördüncü İstekliye göndermektedir
İşlem 5	$Pub(BKTG_i) \rightarrow Pub(İ_1): H_{(taslak\ sözleşme)}$	Proje Birimi kullanıcısı "taslak sözleşme"nin hash değerini beşinci İstekliye göndermektedir

6) İdareye sorulan sorular blok yapısı: İstekliler tarafından, tekliflerini hazırlamak üzere ihale dokümanlarını incelenmesi esnasında İdare'ye soru yöneltilebilmektedir. Bu soruların cevapları sadece soruyu yönelten İstekliye değil, tüm isteklilere gönderilmektedir. Mevcut süreç akışında sorular resmi yazı ile iletilmekte, yazı Proje Yöneticisi onayı ile Teklif Değerlendirme Heyetince cevaplanmaktadır. Uygulama örneğindeyse soruların, cevabın hazırlanarak gönderilmesi işlemlerinde rol alan tüm

taraflara (Proje Yöneticisi ve heyet üyeleri) ayrı ayrı gönderilebilmesi öngörülmüştür. Bu blokta, İdare'ye sorulmuş olan tüm sorulara ilişkin hash değerleri blokzincire kaydedilmektedir. Bu bloğun yapısı Çizelge 5.62'de verilmiştir.

Çizelge 5.62. İdareye sorulan sorular (04) başlıklı beşinci bloğun yapısı

Alan adı	İçerik	Açıklama
Blok bilgileri		
Blok #	4	Beşinci blok
Blok başlığı	H_{BLOK4}	Bloğun hash değeri
Blok Boyutu	… byte	Bloğun byte cinsinden boyutu
Blok konu başlığı	04	"İdareye sorulan sorular" başlığını ifade etmektedir
Önceki bloğun hash değeri	H_{BLOK3}	Önceki bloğun hash değeri
Merkle kökü	$H_{1234567891011…}$	Alt indis olarak verilmiş olan işlemlerin hash değerlerinden elde edilen Merkle kök değerini ifade etmektedir
Zaman damgası	1668506400	Unix Epoch zamanı (Örnek için 15 Kasım 2022 10:00:00 GMT zamanını ifade etmektedir)
İşlem sayısı	30 (5 istekli 6 İdare kull.na)	Bloğun işlemler kısmında yer alan işlem sayısı (İsteklilerce gönderilen soruların hash değerini ifade eden işlemler listelenmektedir)
İşlemler		
İşlem 1	$Pub(İ_1) \rightarrow Pub(PY):H_{(sorular1)}$	Birinci İstekli İdare'ye sorduğu soruların hash değerini Proje Yöneticisine göndermektedir.
İşlem 2	$Pub(İ_1) \rightarrow Pub(TDHB):H_{(sorular1)}$	Birinci İstekli İdare'ye sorduğu soruların hash değerini Teklif Değerlendirme Heyet Başkanına göndermektedir.
İşlem 3	$Pub(İ_1) \rightarrow Pub(TDHÜ_1):H_{(sorular1)}$	Birinci İstekli İdare'ye sorduğu soruların hash değerini Teklif Değerlendirme Heyet Üyesine (1) göndermektedir.
İşlem 4	$Pub(İ_1) \rightarrow Pub(TDHÜ_2):H_{(sorular1)}$	Birinci İstekli İdare'ye sorduğu soruların hash değerini Teklif Değerlendirme Heyet Üyesine (2) göndermektedir.
İşlem 5	$Pub(İ_1) \rightarrow Pub(TDHÜ_3):H_{(sorular1)}$	Birinci İstekli İdare'ye sorduğu soruların hash değerini Teklif Değerlendirme Heyet Üyesine (3) göndermektedir.
İşlem 6	$Pub(İ_1) \rightarrow Pub(TDHÜ_4):H_{(sorular1)}$	Birinci İstekli İdare'ye sorduğu soruların hash değerini Teklif Değerlendirme Heyet Üyesine (4) göndermektedir.
İşlem 7	$Pub(İ_2) \rightarrow Pub(PY):H_{(sorular2)}$	İkinci İstekli İdare'ye sorduğu soruların hash değerini Proje Yöneticisine göndermektedir.
İşlem 8	$Pub(İ_2) \rightarrow Pub(TDHB):H_{(sorular2)}$	İkinci İstekli İdare'ye sorduğu soruların hash değerini Teklif Değerlendirme Heyet Başkanına göndermektedir.
İşlem 9	$Pub(İ_2) \rightarrow Pub(TDHÜ_1):H_{(sorular2)}$	İkinci İstekli İdare'ye sorduğu soruların hash değerini Teklif Değerlendirme Heyet Üyesine (1) göndermektedir.
İşlem 10	$Pub(İ_2) \rightarrow Pub(TDHÜ_2):H_{(sorular2)}$	İkinci İstekli İdare'ye sorduğu soruların hash değerini Teklif Değerlendirme Heyet Üyesine (2) göndermektedir.
İşlem 11	$Pub(İ_2) \rightarrow Pub(TDHÜ_3):H_{(sorular2)}$	İkinci İstekli İdare'ye sorduğu soruların hash değerini Teklif Değerlendirme Heyet Üyesine (3) göndermektedir.
İşlem 12	$Pub(İ_2) \rightarrow Pub(TDHÜ_4):H_{(sorular2)}$	İkinci İstekli İdare'ye sorduğu soruların hash değerini Teklif Değerlendirme Heyet Üyesine (4) göndermektedir.
…	…	…
İşlem 30	$Pub(İ_5) \rightarrow Pub(TDHÜ_4):H_{(sorular5)}$	Beşinci İstekli İdare'ye sorduğu soruların hash değerini Teklif Değerlendirme Heyet Üyesine (4) göndermektedir.

7) İsteklilere verilen cevaplar blok yapısı: İstekliler tarafından sorulan sorulara İdare'nin verdiği cevapların hash değerleri blokzincire bu blokta kaydedilmektedir. Bu bloğun yapısı Çizelge 5.63'te verilmiştir.

Çizelge 5.63. İsteklilere verilen cevaplar (05) başlıklı altıncı bloğun yapısı

Alan adı	İçerik	Açıklama
Blok bilgileri		
Blok #	5	Altıncı blok
Blok başlığı	H_{BLOK5}	Bloğun hash değeri
Blok Boyutu	… byte	Bloğun byte cinsinden boyutu
Blok konu başlığı	05	"İsteklilere verilen cevaplar" başlığını ifade etmektedir
Önceki bloğun hash değeri	H_{BLOK4}	Önceki bloğun hash değeri
Merkle kökü	$H_{1234567891011…}$	Alt indis olarak verilmiş olan işlemlerin hash değerlerinden elde edilen Merkle kök değerini ifade etmektedir
Zaman damgası	1669370400	Unix Epoch zamanı (Örnek için 25 Kasım 2022 10:00:00 GMT zamanını ifade etmektedir)
İşlem sayısı	25 (5 İstekli sorusun cevapları tüm İsteklilere)	Bloğun işlemler kısmında yer alan işlem sayısı
İşlemler		
İşlem 1	$Pub(PY) \rightarrow Pub(İ_1):H_{(cevaplar1)}$	Proje Yöneticisi birinci İstekli sorularının cevabının hash değerini birinci İstekliye göndermektedir.
İşlem 2	$Pub(PY) \rightarrow Pub(İ_2):H_{(cevaplar1)}$	Proje Yöneticisi birinci İstekli sorularının cevabının hash değerini ikinci İstekliye göndermektedir.
İşlem 3	$Pub(PY) \rightarrow Pub(İ_3):H_{(cevaplar1)}$	Proje Yöneticisi birinci İstekli sorularının cevabının hash değerini üçüncü İstekliye göndermektedir.
İşlem 4	$Pub(PY) \rightarrow Pub(İ_4):H_{(cevaplar1)}$	Proje Yöneticisi birinci İstekli sorularının cevabının hash değerini dördüncü İstekliye göndermektedir.
İşlem 5	$Pub(PY) \rightarrow Pub(İ_5):H_{(cevaplar1)}$	Proje Yöneticisi birinci İstekli sorularının cevabının hash değerini beşinci İstekliye göndermektedir.
İşlem 6	$Pub(PY) \rightarrow Pub(İ_1):H_{(cevaplar2)}$	Proje Yöneticisi ikinci İstekli sorularının cevabının hash değerini birinci İstekliye göndermektedir.
İşlem 7	$Pub(PY) \rightarrow Pub(İ_2):H_{(cevaplar2)}$	Proje Yöneticisi ikinci İstekli sorularının cevabının hash değerini ikinci İstekliye göndermektedir.
İşlem 8	$Pub(PY) \rightarrow Pub(İ_3):H_{(cevaplar2)}$	Proje Yöneticisi ikinci İstekli sorularının cevabının hash değerini üçüncü İstekliye göndermektedir.
İşlem 9	$Pub(PY) \rightarrow Pub(İ_4):H_{(cevaplar2)}$	Proje Yöneticisi ikinci İstekli sorularının cevabının hash değerini dördüncü İstekliye göndermektedir.
İşlem 10	$Pub(PY) \rightarrow Pub(İ_5):H_{(cevaplar2)}$	Proje Yöneticisi ikinci İstekli sorularının cevabının hash değerini beşinci İstekliye göndermektedir.
…	…	…
İşlem 25	$Pub(PY) \rightarrow Pub(İ_5):H_{(cevaplar5)}$	Proje Yöneticisi beşinci İstekli sorularının cevabının hash değerini beşinci İstekliye göndermektedir.

8) Geçici Teminat Mektubu blok yapısı: Tekliflerin sunulma süresi bitmeden önce İsteklilerden teklif paketlerini hazırlayarak İdare'ye sunanlar artık Yüklenici Adayı olarak adlandırılmaktadır. Yani, bir İsteklinin teklif vermesi halinde kullandığı açık ve gizli anahtar değişmemektedir. Bununla birlikte, aşağıda verilen blok yapılarında yüklenici adayları için A_i ifadesi kullanılmaktadır. Yüklenici Adayları teklif paketleri içerisinde İdari Şartname, Teknik Şartname ve Taslak Sözleşmeye cevaplarını Geçici Teminat Mektubu, Yetki Belgesi ve Teklif Mektubu ile birlikte sunarlar. Tekliflerin ön değerlendirmesinde bu dokümanların mevcudiyeti ile Geçici Teminat Mektubu, Yetki Belgesi ve Teklif Mektubunun uygunluğu kontrol edilmektedir. Bu kontrollerin daha kolay gerçekleştirilebilmesi, ayrı ayrı blokzincirde kaydedilerek daha sonra daha kolay erişilebilmesi için bu dokümanların her biri ayrı bloklarda tutulmaktadır. Yüklenici

Adayınca sunulan diğer belgeler gibi Geçici Teminat Mektupları da Teklif Değerlendirme Heyetine gönderilmektedir (ihale dokümanları sadece Heyet Üyelerince görülebilecektir). Dokümanların asılları zincir dışında tutulmakta, blokzincirde yalnızca hash değerlerine yer verilmektedir. Buna göre, Geçici Teminat Mektubu bloğunun yapısı Çizelge 5.64'te verilmiştir.

Çizelge 5.64. Geçici Teminat Mektubu (06) başlıklı yedinci bloğun yapısı

Alan adı	İçerik	Açıklama
Blok bilgileri		
Blok #	6	Yedinci blok
Blok başlığı	H_{BLOK6}	Bloğun hash değeri
Blok Boyutu	… byte	Bloğun byte cinsinden boyutu
Blok konu başlığı	06	"Geçici Teminat Mektubu" başlığını ifade etmektedir
Önceki bloğun hash değeri	H_{BLOK5}	Önceki bloğun hash değeri
Merkle kökü	$H_{1234...20}$	Alt indis olarak verilmiş olan işlemlerin hash değerlerinden elde edilen Merkle kök değerini ifade etmektedir
Zaman damgası	1669888800	Unix Epoch zamanı (Örnek için 1 Aralık 2022 10:00:00 GMT zamanını ifade etmektedir)
İşlem sayısı	20 (4 Yüklenici Adayı tarafından 5 Heyet Üyesine)	Bloğun işlemler kısmında yer alan işlem sayısı
İşlemler		
İşlem 1	$Pub(A_1) \rightarrow Pub(TDHB):H_{(GTM1)}$	Birinci Yüklenici Adayı Geçici Teminat Mektubunun hash değerini Teklif Değerlendirme Heyet Başkanına göndermektedir.
İşlem 2	$Pub(A_1) \rightarrow Pub(TDHÜ_1):H_{(GTM1)}$	Birinci Yüklenici Adayı Geçici Teminat Mektubunun hash değerini Teklif Değerlendirme Heyet Üyesine (1) göndermektedir.
İşlem 3	$Pub(A_1) \rightarrow Pub(TDHÜ_2):H_{(GTM1)}$	Birinci Yüklenici Adayı Geçici Teminat Mektubunun hash değerini Teklif Değerlendirme Heyet Üyesine (2) göndermektedir.
İşlem 4	$Pub(A_1) \rightarrow Pub(TDHÜ_3):H_{(GTM1)}$	Birinci Yüklenici Adayı Geçici Teminat Mektubunun hash değerini Teklif Değerlendirme Heyet Üyesine (3) göndermektedir.
İşlem 5	$Pub(A_1) \rightarrow Pub(TDHÜ_4):H_{(GTM1)}$	Birinci Yüklenici Adayı Geçici Teminat Mektubunun hash değerini Teklif Değerlendirme Heyet Üyesine (4) göndermektedir.
İşlem 6	$Pub(A_2) \rightarrow Pub(TDHB):H_{(GTM2)}$	İkinci Yüklenici Adayı Geçici Teminat Mektubunun hash değerini Teklif Değerlendirme Heyet Başkanına göndermektedir.
İşlem 7	$Pub(A_2) \rightarrow Pub(TDHÜ_1):H_{(GTM2)}$	İkinci Yüklenici Adayı Geçici Teminat Mektubunun hash değerini Teklif Değerlendirme Heyet Üyesine (1) göndermektedir.
İşlem 8	$Pub(A_2) \rightarrow Pub(TDHÜ_2):H_{(GTM2)}$	İkinci Yüklenici Adayı Geçici Teminat Mektubunun hash değerini Teklif Değerlendirme Heyet Üyesine (2) göndermektedir.
İşlem 9	$Pub(A_2) \rightarrow Pub(TDHÜ_3):H_{(GTM2)}$	İkinci Yüklenici Adayı Geçici Teminat Mektubunun hash değerini Teklif Değerlendirme Heyet Üyesine (3) göndermektedir.
İşlem 10	$Pub(A_2) \rightarrow Pub(TDHÜ_4):H_{(GTM2)}$	İkinci Yüklenici Adayı Geçici Teminat Mektubunun hash değerini Teklif Değerlendirme Heyet Üyesine (4) göndermektedir.
…	…	…
İşlem 20	$Pub(A_4) \rightarrow Pub(TDHÜ_4):H_{(GTM4)}$	Dördüncü Yüklenici Adayı Geçici Teminat Mektubunun hash değerini Teklif Değerlendirme Heyet Üyesine (4) göndermektedir.

9) Yetki Belgesi blok yapısı: Yüklenici Adayınca teklif vermeye yetkili olunduğuna dair belge de diğer belgeler gibi Teklif Değerlendirme Heyetine gönderilmektedir. Dokümanların asılları zincir dışında tutulmakta, blokzincirde yalnızca hash değerlerine yer verilmektedir. Buna göre, Yetki Belgesi bloğunun yapısı Çizelge 5.65'de verilmiştir.

Çizelge 5.65. Yetki Belgesi (07) başlıklı sekizinci bloğun yapısı

Alan adı	İçerik	Açıklama
Blok bilgileri		
Blok #	7	Sekizinci blok
Blok başlığı	H_{BLOK7}	Bloğun hash değeri
Blok Boyutu	… byte	Bloğun byte cinsinden boyutu
Blok konu başlığı	07	"Yetki Belgesi" başlığını ifade etmektedir
Önceki bloğun hash değeri	H_{BLOK6}	Önceki bloğun hash değeri
Merkle kökü	$H_{1234…20}$	Alt indis olarak verilmiş olan işlemlerin hash değerlerinden elde edilen Merkle kök değerini ifade etmektedir
Zaman damgası	1669888800	Unix Epoch zamanı (Örnek için 1 Aralık 2022 10:00:00 GMT zamanını ifade etmektedir)
İşlem sayısı	20 (4 Yüklenici Adayı 5 Heyet Üyesine)	Bloğun işlemler kısmında yer alan işlem sayısı
İşlemler		
İşlem 1	$Pub(A_1)\rightarrow Pub(TDHB):H_{(YetkiBel1)}$	Birinci Yüklenici Adayı Yetki Belgesinin hash değerini Teklif Değerlendirme Heyet Başkanına göndermektedir.
İşlem 2	$Pub(A_1)\rightarrow Pub(TDHÜ_1):H_{(YetkiBel1)}$	Birinci Yüklenici Adayı Yetki Belgesinin hash değerini Teklif Değerlendirme Heyet Üyesine (1) göndermektedir.
İşlem 3	$Pub(A_1)\rightarrow Pub(TDHÜ_2):H_{(YetkiBel1)}$	Birinci Yüklenici Adayı Yetki Belgesinin hash değerini Teklif Değerlendirme Heyet Üyesine (2) göndermektedir.
İşlem 4	$Pub(A_1)\rightarrow Pub(TDHÜ_3):H_{(YetkiBel1)}$	Birinci Yüklenici Adayı Yetki Belgesinin hash değerini Teklif Değerlendirme Heyet Üyesine (3) göndermektedir.
İşlem 5	$Pub(A_1)\rightarrow Pub(TDHÜ_4):H_{(YetkiBel1)}$	Birinci Yüklenici Adayı Yetki Belgesinin hash değerini Teklif Değerlendirme Heyet Üyesine (4) göndermektedir.
İşlem 6	$Pub(A_2)\rightarrow Pub(TDHB):H_{(YetkiBel2)}$	İkinci Yüklenici Adayı Yetki Belgesinin hash değerini Teklif Değerlendirme Heyet Başkanına göndermektedir.
İşlem 7	$Pub(A_2)\rightarrow Pub(TDHÜ_1):H_{(YetkiBel2)}$	İkinci Yüklenici Adayı Yetki Belgesinin hash değerini Teklif Değerlendirme Heyet Üyesine (1) göndermektedir.
İşlem 8	$Pub(A_2)\rightarrow Pub(TDHÜ_2):H_{(YetkiBel2)}$	İkinci Yüklenici Adayı Yetki Belgesinin hash değerini Teklif Değerlendirme Heyet Üyesine (2) göndermektedir.
İşlem 9	$Pub(A_2)\rightarrow Pub(TDHÜ_3):H_{(YetkiBel2)}$	İkinci Yüklenici Yetki Belgesinin hash değerini Teklif Değerlendirme Heyet Üyesine (3) göndermektedir.
İşlem 10	$Pub(A_2)\rightarrow Pub(TDHÜ_4):H_{(YetkiBel2)}$	İkinci Yüklenici Adayı Yetki Belgesinin hash değerini Teklif Değerlendirme Heyet Üyesine (4) göndermektedir.
…	…	…
İşlem 20	$Pub(A_4)\rightarrow Pub(TDHÜ_4):H_{(YetkiBel4)}$	Dördüncü Yüklenici Adayı Yetki Belgesinin hash değerini Teklif Değerlendirme Heyet Üyesine (4) göndermektedir.

10) Teklif Mektubu blok yapısı: Yüklenici Adayınca teklif tutarı ile teklifin geçerlilik süresini içeren Teklif Mektubu da teklif paketi ile birlikte (mevcut uygulamada kapalı zarf içinde) Teklif Değerlendirme Heyetine gönderilmektedir. Teklif Mektubunun tekliflerin teknik kısımlarının değerlendirilmesi tamamlanmadan açılmaması esastır. Bu nedenle, Teklif Mektubunun ne zaman açılacağına Heyet tarafından karar verilerek bu karar kayıt altına alınmaktadır. Önerilen blokzincir sisteminde de Teklif Mektubunun zincir dışında dijital olarak tutulduğu dikkate alınacak olursa bu dokümana erişim belirli bir süre için engellenmelidir. Bu kontrol süreç içerisinde kullanılacak bir akıllı sözleşme ile gerçekleştirilebileceği gibi zincir dışında tutulan dokümanların şifre ile koruma altına alınması ve erişim şifresinin belirli bir süre kullanılamaması ile sağlanabilir. Diğer bloklarla aynı biçimde, Teklif Mektuplarının da asılları zincir dışında tutulmakta,

blokzincirde yalnızca hash değerlerine yer verilmektedir. Buna göre, Teklif Mektubu bloğunun yapısı Çizelge 5.66'da verilmiştir.

Çizelge 5.66. Teklif Mektubu (08) başlıklı dokuzuncu bloğun yapısı

Alan adı	İçerik	Açıklama
Blok bilgileri		
Blok #	8	Dokuzuncu blok
Blok başlığı	H_{BLOK8}	Bloğun hash değeri
Blok Boyutu	… byte	Bloğun byte cinsinden boyutu
Blok konu başlığı	08	"Teklif Mektubu" başlığını ifade etmektedir
Önceki bloğun hash değeri	H_{BLOK7}	Önceki bloğun hash değeri
Merkle kökü	$H_{1234…20}$	Alt indis olarak verilmiş olan işlemlerin hash değerlerinden elde edilen Merkle kök değerini ifade etmektedir
Zaman damgası	1669888800	Unix Epoch zamanı (Örnek için 1 Aralık 2022 10:00:00 GMT zamanını ifade etmektedir)
İşlem sayısı	20 (4 Yüklenici Adayı 5 Heyet Üyesine)	Bloğun işlemler kısmında yer alan işlem sayısı
İşlemler		
İşlem 1	$Pub(A_1) \rightarrow Pub(TDHB):H_{(TeklMek1)}$	Birinci Yüklenici Adayı Teklif Mektubunun hash değerini Teklif Değerlendirme Heyet Başkanına göndermektedir.
İşlem 2	$Pub(A_1) \rightarrow Pub(TDHÜ_1):H_{(TeklMek1)}$	Birinci Yüklenici Adayı Teklif Mektubunun hash değerini Teklif Değerlendirme Heyet Üyesine (1) göndermektedir.
İşlem 3	$Pub(A_1) \rightarrow Pub(TDHÜ_2):H_{(TeklMek1)}$	Birinci Yüklenici Adayı Teklif Mektubunun hash değerini Teklif Değerlendirme Heyet Üyesine (2) göndermektedir.
İşlem 4	$Pub(A_1) \rightarrow Pub(TDHÜ_3):H_{(TeklMek1)}$	Birinci Yüklenici Adayı Teklif Mektubunun hash değerini Teklif Değerlendirme Heyet Üyesine (3) göndermektedir.
İşlem 5	$Pub(A_1) \rightarrow Pub(TDHÜ_4):H_{(TeklMek1)}$	Birinci Yüklenici Adayı Teklif Mektubunun hash değerini Teklif Değerlendirme Heyet Üyesine (4) göndermektedir.
İşlem 6	$Pub(A_2) \rightarrow Pub(TDHB):H_{(TeklMek2)}$	İkinci Yüklenici Adayı Teklif Mektubunun hash değerini Teklif Değerlendirme Heyet Başkanına göndermektedir.
İşlem 7	$Pub(A_2) \rightarrow Pub(TDHÜ_1):H_{(TeklMek2)}$	İkinci Yüklenici Adayı Teklif Mektubunun hash değerini Teklif Değerlendirme Heyet Üyesine (1) göndermektedir.
İşlem 8	$Pub(A_2) \rightarrow Pub(TDHÜ_2):H_{(TeklMek2)}$	İkinci Yüklenici Adayı Teklif Mektubunun hash değerini Teklif Değerlendirme Heyet Üyesine (2) göndermektedir.
İşlem 9	$Pub(A_2) \rightarrow Pub(TDHÜ_3):H_{(TeklMek2)}$	İkinci Yüklenici Adayı Teklif Mektubunun hash değerini Teklif Değerlendirme Heyet Üyesine (3) göndermektedir.
İşlem 10	$Pub(A_2) \rightarrow Pub(TDHÜ_4):H_{(TeklMek2)}$	İkinci Yüklenici Adayı Teklif Mektubunun hash değerini Teklif Değerlendirme Heyet Üyesine (4) göndermektedir.
…	…	…
İşlem 20	$Pub(A_4) \rightarrow Pub(TDHÜ_4):H_{(TeklMek4)}$	Dördüncü Yüklenici Adayı Teklif Mektubunun hash değerini Teklif Değerlendirme Heyet Üyesine (4) göndermektedir.

11) Tekliflerin İdari kısmının blok yapısı: Yüklenici Adayının İdari Şartnameye cevaplarını içeren dokümanın hash değeri de aynı biçimde Heyet Üyelerine iletilmektedir. İdari şartnameye cevaplar bloğunun yapısı Çizelge 5.67'de verilmiştir.

Çizelge 5.67. Teklifler-İdari (09) başlıklı onuncu bloğun yapısı

Alan adı	İçerik	Açıklama
Blok bilgileri		
Blok #	9	Onuncu blok
Blok başlığı	H_{BLOK9}	Bloğun hash değeri
Blok Boyutu	… byte	Bloğun byte cinsinden boyutu

Blok konu başlığı	09	"Teklifler-İdari" başlığını ifade etmektedir
Önceki bloğun hash değeri	H_{BLOK8}	Önceki bloğun hash değeri
Merkle kökü	$H_{1234\ldots20}$	Alt indis olarak verilmiş olan işlemlerin hash değerlerinden elde edilen Merkle kök değerini ifade etmektedir
Zaman damgası	1669888800	Unix Epoch zamanı (Örnek için 1 Aralık 2022 10:00:00 GMT zamanını ifade etmektedir)
İşlem sayısı	20 (4 Yüklenici Adayı 5 Heyet Üyesine)	Bloğun işlemler kısmında yer alan işlem sayısı
İşlemler		
İşlem 1	$Pub(A_1) \rightarrow Pub(TDHB):H_{(TeklİdariA1)}$	Birinci Yüklenici Adayı İdari Teklifinin hash değerini Teklif Değerlendirme Heyet Başkanına göndermektedir.
İşlem 2	$Pub(A_1) \rightarrow Pub(TDHÜ_1):H_{(TeklİdariA1)}$	Birinci Yüklenici Adayı İdari Teklifinin hash değerini Teklif Değerlendirme Heyet Üyesine (1) göndermektedir.
İşlem 3	$Pub(A_1) \rightarrow Pub(TDHÜ_2):H_{(TeklİdariA1)}$	Birinci Yüklenici Adayı İdari Teklifinin hash değerini Teklif Değerlendirme Heyet Üyesine (2) göndermektedir.
İşlem 4	$Pub(A_1) \rightarrow Pub(TDHÜ_3):H_{(TeklİdariA1)}$	Birinci Yüklenici Adayı İdari Teklifinin hash değerini Teklif Değerlendirme Heyet Üyesine (3) göndermektedir.
İşlem 5	$Pub(A_1) \rightarrow Pub(TDHÜ_4):H_{(TeklİdariA1)}$	Birinci Yüklenici Adayı İdari Teklifinin hash değerini Teklif Değerlendirme Heyet Üyesine (4) göndermektedir.
İşlem 6	$Pub(A_2) \rightarrow Pub(TDHB):H_{(TeklİdariA2)}$	İkinci Yüklenici Adayı İdari Teklifinin hash değerini Teklif Değerlendirme Heyet Başkanına göndermektedir.
İşlem 7	$Pub(A_2) \rightarrow Pub(TDHÜ_1):H_{(TeklİdariA2)}$	İkinci Yüklenici Adayı İdari Teklifinin ubunun hash değerini Teklif Değerlendirme Heyet Üyesine (1) göndermektedir.
İşlem 8	$Pub(A_2) \rightarrow Pub(TDHÜ_2):H_{(TeklİdariA2)}$	İkinci Yüklenici Adayı İdari Teklifinin hash değerini Teklif Değerlendirme Heyet Üyesine (2) göndermektedir.
İşlem 9	$Pub(A_2) \rightarrow Pub(TDHÜ_3):H_{(TeklİdariA2)}$	İkinci Yüklenici Adayı İdari Teklifinin hash değerini Teklif Değerlendirme Heyet Üyesine (3) göndermektedir.
İşlem 10	$Pub(A_2) \rightarrow Pub(TDHÜ_4):H_{(TeklİdariA2)}$	İkinci Yüklenici Adayı İdari Teklifinin tubunun hash değerini Teklif Değerlendirme Heyet Üyesine (4) göndermektedir.
…	…	…
İşlem 20	$Pub(A_4) \rightarrow Pub(TDHÜ_4):H_{(TeklİdariA4)}$	Dördüncü Yüklenici Adayı İdari Teklifinin hash değerini Teklif Değerlendirme Heyet Üyesine (4) göndermektedir.

12) Tekliflerin Teknik kısmının blok yapısı: Yüklenici Adayının Teknik Şartnameye cevaplarını içeren dokümanın hash değeri de aynı biçimde Heyet Üyelerine iletilmektedir. Teknik şartnameye cevaplar bloğunun yapısı Çizelge 5.68'de verilmiştir.

Çizelge 5.68. Teklifler-Teknik (10) başlıklı onbirinci bloğun yapısı

Alan adı	İçerik	Açıklama
Blok bilgileri		
Blok #	10	On birinci blok
Blok başlığı	H_{BLOK10}	Bloğun hash değeri
Blok Boyutu	… byte	Bloğun byte cinsinden boyutu
Blok konu başlığı	10	"Teklifler-Teknik" başlığını ifade etmektedir
Önceki bloğun hash değeri	H_{BLOK9}	Önceki bloğun hash değeri
Merkle kökü	$H_{1234\ldots20}$	Alt indis olarak verilmiş olan işlemlerin hash değerlerinden elde edilen Merkle kök değerini ifade etmektedir
Zaman damgası	1669888800	Unix Epoch zamanı (Örnek için 1 Aralık 2022 10:00:00 GMT zamanını ifade etmektedir)
İşlem sayısı	20 (4 Yüklenici Adayı 5 Heyet Üyesine)	Bloğun işlemler kısmında yer alan işlem sayısı
İşlemler		
İşlem 1	$Pub(A_1) \rightarrow Pub(TDHB):H_{(TeklTeknikA1)}$	Birinci Yüklenici Adayı Teknik Teklifinin hash değerini Teklif Değerlendirme Heyet Başkanına göndermektedir.
İşlem 2	$Pub(A_1) \rightarrow Pub(TDHÜ_1):H_{(TeklTeknikA1)}$	Birinci Yüklenici Adayı Teknik Teklifinin hash değerini Teklif Değerlendirme Heyet Üyesine (1) göndermektedir.

İşlem 3	$Pub(A_1) \rightarrow Pub(TDHÜ_2):H_{(TeklTeknik1)}$	Birinci Yüklenici Adayı Teknik Teklifinin hash değerini Teklif Değerlendirme Heyet Üyesine (2) göndermektedir.
İşlem 4	$Pub(A_1) \rightarrow Pub(TDHÜ_3):H_{(TeklTeknik1)}$	Birinci Yüklenici Adayı Teknik Teklifinin hash değerini Teklif Değerlendirme Heyet Üyesine (3) göndermektedir.
İşlem 5	$Pub(A_1) \rightarrow Pub(TDHÜ_4):H_{(TeklTeknik1)}$	Birinci Yüklenici Adayı Teknik Teklifinin hash değerini Teklif Değerlendirme Heyet Üyesine (4) göndermektedir.
İşlem 6	$Pub(A_2) \rightarrow Pub(TDHB):H_{(TeklTeknik2)}$	İkinci Yüklenici Adayı Teknik Teklifinin hash değerini Teklif Değerlendirme Heyet Başkanına göndermektedir.
İşlem 7	$Pub(A_2) \rightarrow Pub(TDHÜ_1):H_{(TeklTeknik2)}$	İkinci Yüklenici Adayı Teknik Teklifinin ubunun hash değerini Teklif Değerlendirme Heyet Üyesine (1) göndermektedir.
İşlem 8	$Pub(A_2) \rightarrow Pub(TDHÜ_2):H_{(TeklTeknik2)}$	İkinci Yüklenici Adayı Teknik Teklifinin hash değerini Teklif Değerlendirme Heyet Üyesine (2) göndermektedir.
İşlem 9	$Pub(A_2) \rightarrow Pub(TDHÜ_3):H_{(TeklTeknik2)}$	İkinci Yüklenici Adayı Teknik Teklifinin hash değerini Teklif Değerlendirme Heyet Üyesine (3) göndermektedir.
İşlem 10	$Pub(A_2) \rightarrow Pub(TDHÜ_4):H_{(TeklTeknik2)}$	İkinci Yüklenici Adayı Teknik Teklifinin tubunun hash değerini Teklif Değerlendirme Heyet Üyesine (4) göndermektedir.
…	…	…
İşlem 20	$Pub(A_4) \rightarrow Pub(TDHÜ_4):H_{(TeklTeknik4)}$	Dördüncü Yüklenici Adayı Teknik Teklifinin hash değerini Teklif Değerlendirme Heyet Üyesine (4) göndermektedir.

13) Tekliflerin Taslak Sözleşme kısmının blok yapısı: Yüklenici Adayının Taslak Sözleşmeye cevaplarını içeren dokümanın hash değeri de aynı biçimde Heyet Üyelerine iletilmektedir. Teknik şartnameye cevaplar bloğunun yapısı Çizelge 5.69'de verilmiştir.

Çizelge 5.69. Teklifler-Taslak Sözleşme (11) başlıklı onikinci bloğun yapısı

Alan adı	İçerik	Açıklama
Blok bilgileri		
Blok #	11	On ikinci blok
Blok başlığı	H_{BLOK11}	Bloğun hash değeri
Blok Boyutu	… byte	Bloğun byte cinsinden boyutu
Blok konu başlığı	11	"Teklifler-Teknik" başlığını ifade etmektedir
Önceki bloğun hash değeri	H_{BLOK10}	Önceki bloğun hash değeri
Merkle kökü	$H_{1234…20}$	Alt indis olarak verilmiş olan işlemlerin hash değerlerinden elde edilen Merkle kök değerini ifade etmektedir
Zaman damgası	1669888800	Unix Epoch zamanı (Örnek için 1 Aralık 2022 10:00:00 GMT zamanını ifade etmektedir)
İşlem sayısı	20 (4 Yüklenici Adayı 5 Heyet Üyesine)	Bloğun işlemler kısmında yer alan işlem sayısı
İşlemler		
İşlem 1	$Pub(A_1) \rightarrow Pub(TDHB):H_{(TeklSözl1)}$	Birinci Yüklenici Adayı Taslak Sözleşmeye cevaplarının hash değerini Teklif Değerlendirme Heyet Başkanına göndermektedir.
İşlem 2	$Pub(A_1) \rightarrow Pub(TDHÜ_1):H_{(TeklSözl1)}$	Birinci Yüklenici Adayı Taslak Sözleşmeye cevaplarının hash değerini Teklif Değerlendirme Heyet Üyesine (1) göndermektedir.
İşlem 3	$Pub(A_1) \rightarrow Pub(TDHÜ_2):H_{(TeklSözl1)}$	Birinci Yüklenici Adayı Taslak Sözleşmeye cevaplarının hash değerini Teklif Değerlendirme Heyet Üyesine (2) göndermektedir.
İşlem 4	$Pub(A_1) \rightarrow Pub(TDHÜ_3):H_{(TeklSözl1)}$	Birinci Yüklenici Adayı Taslak Sözleşmeye cevaplarının hash değerini Teklif Değerlendirme Heyet Üyesine (3) göndermektedir.
İşlem 5	$Pub(A_1) \rightarrow Pub(TDHÜ_4):H_{(TeklSözl1)}$	Birinci Yüklenici Adayı Taslak Sözleşmeye cevaplarının hash değerini Teklif Değerlendirme Heyet Üyesine (4) göndermektedir.
İşlem 6	$Pub(A_2) \rightarrow Pub(TDHB):H_{(TeklSözl2)}$	İkinci Yüklenici Adayı Taslak Sözleşmeye cevaplarının hash değerini Teklif Değerlendirme Heyet Başkanına göndermektedir.
İşlem 7	$Pub(A_2) \rightarrow Pub(TDHÜ_1):H_{(TeklSözl2)}$	İkinci Yüklenici Adayı Taslak Sözleşmeye cevaplarının hash değerini Teklif Değerlendirme Heyet Üyesine (1) göndermektedir.
İşlem 8	$Pub(A_2) \rightarrow Pub(TDHÜ_2):H_{(TeklSözl2)}$	İkinci Yüklenici Adayı Taslak Sözleşmeye cevaplarının hash değerini Teklif Değerlendirme Heyet Üyesine (2) göndermektedir.
İşlem 9	$Pub(A_2) \rightarrow Pub(TDHÜ_3):H_{(TeklSözl2)}$	İkinci Yüklenici Adayı Taslak Sözleşmeye cevaplarının hash değerini Teklif Değerlendirme Heyet Üyesine (3) göndermektedir.

İşlem 10	$Pub(A_2) \rightarrow Pub(TDHÜ_4):H_{(TeklSözl2)}$	İkinci Yüklenici Adayı Taslak Sözleşmeye cevaplarının tubunun hash değerini Teklif Değerlendirme Heyet Üyesine (4) göndermektedir.
…	…	…
İşlem 20	$Pub(A_4) \rightarrow Pub(TDHÜ_4):H_{(TeklSözl4)}$	Dördüncü Yüklenici Adayı Taslak Sözleşmeye cevaplarının hash değerini Teklif Değerlendirme Heyet Üyesine (4) göndermektedir.

14) Yüklenici adaylarına sorulan sorular blok yapısı: Tekliflerin değerlendirilmesi aşamasında, tekliflerde detaylandırılması istenen, anlaşılamayan ya da teyit gerektiren konular Yüklenici Adaylarına soru olarak yöneltilebilmektedir. Teklif Değerlendirme Heyetince belirlenen bu sorular yüklenici adayına Proje Yöneticisi onayı ile gönderilmektedir. İdare'nin Yüklenici Adaylarına sorduğu soruların hash değerleri blokzincire bu blokta kaydedilmektedir. Bu bloğun yapısı Çizelge 5.70'te verilmiştir.

Çizelge 5.70. Yüklenici adaylarına sorulan sorular (12) başlıklı onüçüncü bloğun yapısı

Alan adı	İçerik	Açıklama
Blok bilgileri		
Blok #	12	On üçüncü blok
Blok başlığı	H_{BLOK12}	Bloğun hash değeri
Blok Boyutu	… byte	Bloğun byte cinsinden boyutu
Blok konu başlığı	12	"Yüklenici adaylarına sorulan sorular" başlığını ifade etmektedir
Önceki bloğun hash değeri	H_{BLOK11}	Önceki bloğun hash değeri
Merkle kökü	H_{1234}	Alt indis olarak verilmiş olan işlemlerin hash değerlerinden elde edilen Merkle kök değerini ifade etmektedir
Zaman damgası	1671098400	Unix Epoch zamanı (Örnek için 15 Aralık 2022 10:00:00 GMT zamanını ifade etmektedir)
İşlem sayısı	4	Bloğun işlemler kısmında yer alan işlem sayısı (İdarece gönderilen soruların hash değerini ifade eden işlemler listelenmektedir)
İşlemler		
İşlem 1	$Pub(PY) \rightarrow Pub(A_1):H_{(sorularİdare1)}$	Proje Yöneticisi birinci Yüklenici Adayına sorularının hash değerini göndermektedir.
İşlem 2	$Pub(PY) \rightarrow Pub(A_2):H_{(sorularİdare2)}$	Proje Yöneticisi ikinci Yüklenici Adayına sorularının hash değerini göndermektedir.
İşlem 3	$Pub(PY) \rightarrow Pub(A_3):H_{(sorularİdare3)}$	Proje Yöneticisi üçüncü Yüklenici Adayına sorularının hash değerini göndermektedir.
İşlem 4	$Pub(PY) \rightarrow Pub(A_4):H_{(sorularİdare4)}$	Proje Yöneticisi dördüncü Yüklenici Adayına sorularının hash değerini göndermektedir.

15) İdareye verilen cevaplar blok yapısı: İdare tarafından sorulan soruların cevapları yüklenici adaylarınca Proje Yöneticisi ve heyet üyelerine ayrı ayrı gönderilmektedir. Bu blokta, İdare tarafından sorulmuş olan soruların cevaplarına ilişkin hash değerleri blokzincire kaydedilmektedir. Bu bloğun yapısı Çizelge 5.71'de verilmiştir.

Çizelge 5.71. İdareye verilen cevaplar (13) başlıklı ondördüncü bloğun yapısı

Alan adı	İçerik	Açıklama
Blok bilgileri		
Blok #	13	On dördüncü blok
Blok başlığı	H_{BLOK13}	Bloğun hash değeri

Blok Boyutu	… byte	Bloğun byte cinsinden boyutu
Blok konu başlığı	13	"İdareye verilen cevaplar" başlığını ifade etmektedir
Önceki bloğun hash değeri	H_{BLOK12}	Önceki bloğun hash değeri
Merkle kökü	$H_{1234...24}$	Alt indis olarak verilmiş olan işlemlerin hash değerlerinden elde edilen Merkle kök değerini ifade etmektedir
Zaman damgası	1671530400	Unix Epoch zamanı (Örnek için 20 Aralık 2022 10:00:00 GMT zamanını ifade etmektedir)
İşlem sayısı	24 (4 yüklenici adayı tarafından 6 idare kullanıcısına)	Bloğun işlemler kısmında yer alan işlem sayısı (Yüklenici adaylarınca gönderilen cevapların hash değerini ifade eden işlemler listelenmektedir)
İşlemler		
İşlem 1	$Pub(A_1) \rightarrow Pub(PY):H_{(cevaplarAday1)}$	Birinci Yüklenici Adayı cevaplarının hash değerini Proje Yöneticisine göndermektedir.
İşlem 2	$Pub(A_1) \rightarrow Pub(TDHB):H_{(cevaplarAday1)}$	Birinci Yüklenici Adayı cevaplarının hash değerini Teklif Değerlendirme Heyet Başkanına göndermektedir.
İşlem 3	$Pub(A_1) \rightarrow Pub(TDHÜ_1):H_{(cevaplarAday1)}$	Birinci Yüklenici Adayı cevaplarının hash değerini Teklif Değerlendirme Heyet Üyesine (1) göndermektedir.
İşlem 4	$Pub(A_1) \rightarrow Pub(TDHÜ_2):H_{(cevaplarAday1)}$	Birinci Yüklenici Adayı cevaplarının hash değerini Teklif Değerlendirme Heyet Üyesine (2) göndermektedir.
İşlem 5	$Pub(A_1) \rightarrow Pub(TDHÜ_3):H_{(cevaplarAday1)}$	Birinci Yüklenici Adayı cevaplarının hash değerini Teklif Değerlendirme Heyet Üyesine (3) göndermektedir.
İşlem 6	$Pub(A_1) \rightarrow Pub(TDHÜ_4):H_{(cevaplarAday1)}$	Birinci Yüklenici Adayı cevaplarının hash değerini Teklif Değerlendirme Heyet Üyesine (4) göndermektedir.
İşlem 7	$Pub(A_2) \rightarrow Pub(PY):H_{(cevaplarAday2)}$	İkinci Yüklenici Adayı cevaplarının hash değerini Proje Yöneticisine göndermektedir.
İşlem 8	$Pub(A_2) \rightarrow Pub(TDHB):H_{(cevaplarAday2)}$	İkinci Yüklenici Adayı cevaplarının hash değerini Teklif Değerlendirme Heyet Başkanına göndermektedir.
İşlem 9	$Pub(A_2) \rightarrow Pub(TDHÜ_1):H_{(cevaplarAday2)}$	İkinci Yüklenici Adayı cevaplarının hash değerini Teklif Değerlendirme Heyet Üyesine (1) göndermektedir.
İşlem 10	$Pub(A_2) \rightarrow Pub(TDHÜ_2):H_{(cevaplarAday2)}$	İkinci Yüklenici Adayı cevaplarının hash değerini Teklif Değerlendirme Heyet Üyesine (2) göndermektedir.
İşlem 11	$Pub(A_2) \rightarrow Pub(TDHÜ_3):H_{(cevaplarAday2)}$	İkinci Yüklenici Adayı cevaplarının hash değerini Teklif Değerlendirme Heyet Üyesine (3) göndermektedir.
İşlem 12	$Pub(A_2) \rightarrow Pub(TDHÜ_4):H_{(cevaplarAday2)}$	İkinci Yüklenici Adayı cevaplarının hash değerini Teklif Değerlendirme Heyet Üyesine (4) göndermektedir.
…	…	…
İşlem 24	$Pub(A_4) \rightarrow Pub(TDHÜ_4):H_{(cevaplarAday4)}$	Dördüncü Yüklenici Adayı cevaplarının hash değerini Teklif Değerlendirme Heyet Üyesine (4) göndermektedir.

16) Teklif Değerlendirme Sonuç Raporu blok yapısı: Teklif Değerlendirme Heyetinin değerlendirme sonuçları Heyet Üyelerince rapor haline getirilerek Proje Yöneticisine sunulmakta, Proje Yöneticisi onayı ile de nihai olarak Üst Yöneticiye arz edilmektedir. Uygulama örneğinin süreç akışında ilk değerlendirme sonrasında Yüklenici Adaylarından En İyi ve En Son Tekliflerin alınması, buna göre tekliflerin yeniden değerlendirilmesi, en sonunda da Üst Yönetici kararı ile Fiyat Yenileme istenerek tekliflerin son değerlendirmesi ile Yüklenici kararının verilmesi işlemleri tarif edilmekle birlikte, blok yapısında bu adımlar gösterilmemiş, doğrudan Teklif Değerlendirme Sonuç Raporunun sunumuna geçilmiştir. Bu blokta, Teklif Değerlendirme Sonuç Raporunun hash değeri blokzincire kaydedilmektedir. Bu bloğun yapısı Çizelge 5.72'de verilmiştir.

Çizelge 5.72. Teklif Değerlendirme Sonuç Raporu (14) başlıklı onbeşinci bloğun yapısı

Alan adı	İçerik	Açıklama
Blok bilgileri		
Blok #	14	On beşinci blok
Blok başlığı	H_{BLOK14}	Bloğun hash değeri
Blok Boyutu	… byte	Bloğun byte cinsinden boyutu
Blok konu başlığı	14	"Teklif Değerlendirme Sonuç Raporu" başlığını ifade etmektedir
Önceki bloğun hash değeri	H_{BLOK13}	Önceki bloğun hash değeri
Merkle kökü	H_{12}	Alt indis olarak verilmiş olan işlemlerin hash değerlerinden elde edilen Merkle kök değerini ifade etmektedir
Zaman damgası	1671962400	Unix Epoch zamanı (Örnek için 25 Aralık 2022 10:00:00 GMT zamanını ifade etmektedir)
İşlem sayısı	2	Bloğun işlemler kısmında yer alan işlem sayısı
İşlemler		
İşlem 1	Pub(TDHB)→Pub(PY):$H_{(TDSR)}$	Teklif Değerlendirme Heyet Başkanı Teklif Değerlendirme Sonuç Raporunun hash değerini Proje Yöneticisine göndermektedir.
İşlem 2	Pub(PY)→Pub(ÜY):$H_{(TDSR)}$	Proje Yöneticisi Teklif Değerlendirme Sonuç Raporunun hash değerini Üst Yöneticiye göndermektedir.

17) Yüklenici Seçim Kararı blok yapısı: Teklif Değerlendirme Sonuç Raporunun sunularak onaylanmasının ardından değerlendirme sonucuna göre en uygun teklifi sunmuş olan Yüklenici Adayı Yüklenici olarak tüm Yüklenici Adaylarına ve İhale Birimi Kullanıcı(lar)ına bildirilir. Bu bildirim Üst Yönetici tarafından yapılmaktadır. Bu örnekte, birinci Yüklenici Adayının seçildiği varsayılmış, blok içerisinde Yüklenici Adayı (A_1) yerine "Y" kullanıcısına yer verilmiştir. Bu blokta, Yüklenici Seçim Kararının hash değeri blokzincire kaydedilmektedir. Bu bloğun yapısı Çizelge 5.73'te verilmiştir.

Çizelge 5.73. Yüklenici Seçim Kararı (15) başlıklı onbeşinci bloğun yapısı

Alan adı	İçerik	Açıklama
Blok bilgileri		
Blok #	15	On altıncı blok
Blok başlığı	H_{BLOK15}	Bloğun hash değeri
Blok Boyutu	… byte	Bloğun byte cinsinden boyutu
Blok konu başlığı	15	"Yüklenici Seçim Kararı" başlığını ifade etmektedir
Önceki bloğun hash değeri	H_{BLOK14}	Önceki bloğun hash değeri
Merkle kökü	H_{12}	Alt indis olarak verilmiş olan işlemlerin hash değerlerinden elde edilen Merkle kök değerini ifade etmektedir
Zaman damgası	1672394400	Unix Epoch zamanı (Örnek için 30 Aralık 2022 10:00:00 GMT zamanını ifade etmektedir)
İşlem sayısı	2	Bloğun işlemler kısmında yer alan işlem sayısı
İşlemler		
İşlem 1	Pub(ÜY)→Pub($İBK_1$):$H_{(YSK)}$	Üst Yönetici Yüklenici Seçim Kararının hash değerini İhale Birimi Kullanıcısına (1) göndermektedir.
İşlem 2	Pub(ÜY)→Pub($İBK_2$):$H_{(YSK)}$	Üst Yönetici Yüklenici Seçim Kararının hash değerini İhale Birimi Kullanıcısına (2) göndermektedir.
İşlem 3	Pub(ÜY)→Pub(Y):$H_{(YSK)}$	Üst Yönetici Yüklenici Seçim Kararının hash değerini Yükleniciye (birinci Yüklenici Adayı) göndermektedir.

İşlem 4	Pub(ÜY)→Pub(A_2):$H_{(YSK)}$	Üst Yönetici Yüklenici Seçim Kararının hash değerini ikinci Yüklenici Adayına göndermektedir.
İşlem 5	Pub(ÜY)→Pub(A_3):$H_{(YSK)}$	Üst Yönetici Yüklenici Seçim Kararının hash değerini üçüncü Yüklenici Adayına göndermektedir.
İşlem 6	Pub(ÜY)→Pub(A_4):$H_{(YSK)}$	Üst Yönetici Yüklenici Seçim Kararının hash değerini dördüncü Yüklenici Adayına göndermektedir.

Hassas, gizli ya da kritik veri ya da bilgi kullanımı

Blokzincir ağında ihale sürecine ilişkin dokümanların hash değerleri kaydedildiğinden verilerin içeriği erişilebilir değildir. Bununla birlikte, zincir dışı ağda tutulan verilerin gizlilik durumları ile kişisel veri içerip içermedikleri Ek-2 Süreç Bilgi Formunun dokuzuncu maddesinde verilmiştir. Ancak, burada dikkate alınması gereken konu sistemdeki kullanıcıların kullandıkları anahtarlardır. Tek bir ihale için kullanıldığında sorun yaratmamakla birlikte, bloklar içerisindeki tüm işlemler bu adresler ile gerçekleştirildiğinden, ihale sonuçları duyurulduktan sonra kullanıcılarla kullanıcı anahtarları arasında eşleştirme yapılması mümkündür. Şöyle ki, Yüklenici Seçim Kararı ile duyurulan yüklenicinin adresi kullanılarak önceki bloklarda bu yükleniciye ait diğer işlemlerin analizi yapılabilir. Aynı biçimde, Üst Yönetici, Proje Yöneticisi ya da Heyet Üyelerinin anahtarları da daha sonraki ihalelerde kullanılmaları halinde anahtar-kullanıcı eşleşmesi kolaylıkla yapılabilecektir. Bu nedenle, kullanıcı anonimliğinin sağlanması için her bir ihale için farklı anahtar üretilmesi ya da blokzincir tasarımında sıfır bilgi ispatı (zero-knowledge proof) gibi tekniklerin kullanılması önerilmektedir.

Dış bilgi

Süreç içerisinde banka dekontu, geçici teminat mektubu, yetki belgesi gibi dış dokümanlar kullanılmakla birlikte bunların tamamı teklif paketi içerisinde değerlendirilmektedir. Bloklar içerisinde bahse konu dış bilgilerin hash değerlerine yer verilmekte olup sisteme veri sağlayan sensör vb. dış kaynak bulunmamaktadır.

5.5.2. Öncelik sırasına göre ilk sıradaki platformun özellikleri

Seçilen uygulama konusu (Kamu İhale Süreci) için kritik olan özellikler gizlilik ve güvenlik, şeffaflık, hesap verebilirlik olup sürecin kurum içinden ve dışından paydaşlarının olması, mevcut durumda gizlilik ve güvenliğin manuel kontrollere bağlı olması, süreçte rol alan tarafların yetkileri ve sorumluluklarının farklılığı, erişim izinlerinin düzenlenmesi ve

takibinin güçlüğü, şeffaflığının sınırlı düzeyde olması ve manuel işlemler nedeniyle tamamlanma süresinde iyileştirilebilir alanlar içermesi gibi nedenlerle blokzincir teknolojisinin kullanımına uygun olduğu değerlendirilmektedir.

Bu kapsamda, süreç için fonksiyonel olmayan özelliklerden sistem güvenliği, mevzuata uyum ve şeffaflığın önem düzeyi yüksek olarak tanımlanmıştır. Sistemden beklenen diğer önemli özellikler ise blokzincir ağına katılımın izne bağlı olması (özel blokzincir), akıllı sözleşme desteğinin bulunması, DDoS saldırılarına, Sybil saldırılarına ve kuantum bilişim riskine karşı direncinin yüksek olması, kullanılacak platformun güvenilirlik, olgunluk ve pazardaki itibarının yüksek olmasıdır. Bu özellikler dikkate alınarak platform alternatifleri birbirleri ile karşılaştırılmış, tasarlanan sistem için en uygun alternatifin Hyperledger, en uygun ikinci alternatifin ise Corda platformu olduğu tespit edilmiştir.

Tezin İkinci Bölümündeki platform özellikleri konusunda detaylarına yer verildiği üzere, Hyperledger platformunun Fabric, Sawtooth, Iroha ve Indy olmak üzere başlıca dört türü bulunmaktadır. Bunlardan Fabric çoklu kayıt defteri yapısı, aynı ağ üzerinde özel kanalları kullanabilmesi, Üyelik Hizmeti Sağlayıcısı (MSP) özellikleri ile Hyperledger'ın kurumsal uygulamalar için en yaygın biçimde kullanılan tipidir. Sawtooth daha çok performans sorunlarının giderilmesi için geliştirilmiş olan versiyon olup uygulama örneğinde işlem hacmi ve işlem hızı çok önemli bileşenler olmadığından herhangi bir performans problemi öngörülmemektedir. Iroha karmaşık dijital varlıklar ve kimlik yönetimi için, Indy ise merkeziyetsiz kimlik yönetimi için geliştirilmiştir. Bu özellikleri dikkate alınarak, Kamu İhale Süreci için en uygun Hyperledger tipinin Fabric olduğu değerlendirilmektedir.

Özel blokzincir, her bir düğümün yazma izinlerinin iç kontrole tabi olduğu, okuma izinlerinin ise gerektiğinde seçici olarak dışarıya açıldığı, halka açık olmayan bir zincirdir. Hyperledger Fabric platformunda, tüm katılımcıların blokzincirdeki işleme katılabilmeleri için kimliklerinin doğrulanması gerekir. Hyperledger Fabric ayrıca sistemin uygulama mantığını tanımlayan ve yürüten akıllı sözleşmeleri destekler. Hyperledger'da tüm zincir kodları Docker konteynırında[13] çalışır. Konteynırdaki farklı bileşenlerin ve zincir kodlarının modüler yapısı esneklik, çok yönlülük ve yeniden kullanılabilirlik özelliklerini sağlar.

[13] Uygulamanın bir bilgisayar ortamından diğerine hızlı ve güvenilir bir şekilde çalışması için kodu ve tüm bağımlılıklarını paketleyen standart bir yazılım birimidir.

Hyperledger Fabric'te farklı hizmetlerin farklı kanallarda çalışmasını ve kanala bağlı düğümler arasında veri izolasyonunu sağlayan çok kanallı (multichannel) kavramı da kullanılmaktadır. Bu çoklu kanal yapısı ile kullanıcılar birbirlerinden izole edilebilmekte, böylelikle gizlilik ve güvenlik daha kolay bir biçimde sağlanabilmektedir. Hyperledger'ın bu özelliği birbirleri hakkında bilgi sahibi olması istenmeyen yüklenici adayları, teknik değerlendirme tamamlanmadan görülmemesi gereken fiyat bilgileri gibi konuları nedeniyle ihale süreci için büyük avantaj sağlamaktadır.

Hyperledger Fabric'in esnek ve modüler yapısı bir diğer avantajı olup önemli özellikleri aşağıdaki biçimde sıralanabilir:

- Chaincode: Ethereum ağındaki akıllı sözleşmelere benzeyen ancak daha gelişmiş bir dilde yazılmış komut dosyasıdır. Yürütülen tüm işlemler tüm katılımcıların bilgileri görebileceği bir defterde kalıcı olarak tutulur. Chaincode aslında iş mantığını yöneten akıllı sözleşmeleri yöneten bir üst kümedir.
- Kanal yapısı: Gizli verileri birden çok ağ üyesi arasında aktarmak için kullanılan özel bir iletişim alt ağıdır. Bir kanaldaki etkinliklerin sadece ilişkili ve yetkili kuruluşlar tarafından görülebilmesini sağlar.
- Üyelik hizmeti sağlayıcısı (MSP): MSP güven alanının üyelerini tanımlamak, sertifika yayınlayarak ve bunları doğrulayarak kimlik doğrulamayı ve erişim kontrolünü sağlamak ve üyelerin blokzincir ağında sahip olabileceği üye, yönetici gibi belirli rolleri belirlemek için güvenilir bir Sertifika Yetkilisini (CA) tanımlamak için kullanılmaktadır.
- Idemix (Identity mixer): IBM Research tarafından geliştirilen bir dizi protokol şifreleme bileşeni, anonim bir kimlik bilgisi teknolojisidir. Idemix ile istemcinin gerçek kimliğini gizlemek için hem güçlü bir kimlik doğrulama hem de gizlilik koruması uygulanabilmekte olup başlıca iki özelliği:
    - İstemcinin kimliği ifşa edilmeden işlemlerin gerçekleştirilmesine olanak sağlayan bir işlev olan anonimlik,
    - Bu işlemlerin aynı kimlik tarafından gerçekleştirildiğini göstermeden tek bir kimlikle birden fazla işlemin gönderilmesini sağlayan bağlantısızlık biçimindedir.

  Idemix sürecinde kullanıcı, yayınlayan (issuer) ve doğrulayıcı (verifier) olmak üzere üç rol bulunmaktadır. Bu teknoloji kör imza şemasına dayanmaktadır. İşlemlerde kişisel verilerin gizlenmesini en üst düzeye çıkarmak için birden fazla mesaj içeren imzaları ve geçerli sıfır bilgi kanıtlarını desteklemektedir. Bu nedenle, ihale sürecinde kullanıcıların

sistem kimliklerinin gizlenmesi ve anonim giriş gerçekleştirilebilmesi istendiğinde Idemix'ten faydalanılabilecektir.

Hyperledger Fabric tabanlı blokzincir ağı temelde birkaç farklı unsurdan oluşmaktadır:

1) Ağdaki kuruluşların (İdare ve Yüklenici Adayları) her biri, paylaşılan kayıt defterleri ve zincir kodunu barındıran bir ağda temel rolleri yürüten birkaç eşe sahiptir,
2) Belirli bir ihale sürecinde yer alan kuruluşların özel ve gizli işlemlerini yürütmek amacıyla hepsini birbirine bağlamak için tek bir ortak kanal oluşturulur,
3) Ayrı bir Hyperledger Fabric Sertifika Yetkilisi ağ üyesi kullanıcılara PKI tabanlı sertifikalar vermek üzere kullanılır,
4) Sistemin Üyelik Hizmet Sağlayıcısı bileşeni ağa katılabilmeleri için istemcilerin ve eşlerin kimlik bilgilerini eşleştirmek için kullanılır,
5) İdare tüm onaylayan düğümlerden işlemleri alır, bunları bloklar halinde düzenler, son olarak da nihai doğrulama için eşlere dağıtır ve kayıt defterine kaydeder,
6) İstekli ya da yüklenici adayı olarak tanımlanan kullanıcılar işlem tekliflerini tetikleyen uygulama aracılığı ile blokzincir ağına işlemlerini gönderir,
7) Zincir kodu onay eşi adı verilen, ilgili İdare kullanıcısı düğümünde yürütülür, yürütmenin sonucu onaylayan eş tarafından imzalanan işlem yanıtı olarak deftere kaydedilmeyen bir kümede toplanır,
8) Onaylayan eş tarafından imzalanmış işlemler onay politikasına dayalı bir fikir birliğine varmak üzere karşılaştırılır,
9) Fikir birliğine ulaşılması ya da tek onay makamı olması halinde bu kullanıcı tarafından onay verilmesi halinde işlem teklifi İdare'ye gönderilir.
10) Fikir birliğine ulaşılamaması halinde işlem yine de iletilir ancak ilgilisi tarafından kayıt defterinde "geçersiz" olarak işaretlenir.
11) Tüm işlemler ilgili blok içerisinde toplandıktan sonra bunlar kanaldaki taahhüt makamını temsil eden kullanıcı eşine iletilir,
12) Bu kullanıcılar bloklar içerisindeki işlemleri doğrular ve blok böylece zincire eklenir,
13) Tüm geçersiz ya da başarısız işlemler de denetim amacıyla blokzincirde yer alır.

Kamu ihale süreci için en uygun olduğu değerlendirilen iki platformun (Hyperledger Fabric ve Corda) detayları tezin İkinci Bölümünde verilmiş olan temel özellikleri Çizelge 5.74'te özetlenmiştir.

Çizelge 5.74. Hyperledger Fabric ve Corda platformlarının temel özellikleri

Özellik	Hyperledger (Fabric)	Corda
Ağa katılım	İzin gerektiren	İzin gerektiren
Blokzincir tipi	Özel	Özel
Hash fonksiyonu	SHA-256	SHA256withRSA, SHA256withECDSA ve BPQS
Mutabakat mekanizması	İzin gerektiren, oylamaya dayalı bir algoritma olan Apache Kafka kullanılmaktadır	Herhangi bir mutabakat algoritmasına bağımlı değildir.
Yazılım dili	Python, Go, Rust, JavaScript ve Java	Kotlin, Java, C++, Python, Groovy, Shell
Yazılım tipi	Açık kaynaklı, modüler ve yapılandırılabilir bir mimari	Açık kaynak kodlu olarak Github'da sunulmaktadır.
İşlem hacmi (saniyede)	> 3 500, Yüksek	Çok yüksek (20 000'e kadar çıkabilmektedir)
Ağ gecikmesi	İşlemler birkaç saniye içinde kesinleşmektedir	Çok düşük
Ölçeklenebilirlik	Yüksek	Yüksek
İşlem hızı	Çok hızlı	Çok hızlı
Blokzincir üçlü çelişkisi	"Merkezsizlik" düşük	"Merkezsizlik" düşük
DoS&DDoS saldırılarına direnç	Yüksek	Yüksek
Sybil saldırısına direnç	Yüksek	Yüksek
Kuantum bilişim riskine direnç	Düşük	BPQS (Blockchained Post-Quantum Signatures) ile dirençli
Mahremiyet ve gizlilik teknolojisi	Yüksek	Veriler, bilmesi gereken (need-to-know) bir temelde paylaşılır
Uygulama türü	Kurumsal uygulamalar	Daha çok bankalar için gizlilik ve güvenlik konularına odaklanmıştır
Akıllı sözleşme desteği	Var – Chaincode	Var - CorDapps
Akıllı sözleşme dil desteği	JavaScript, Java, Go ve Node.js	CorDapp Design Language (CDL)
Token kullanımı	Tokendan bağımsız	Mümkün
Olgunluk	Yüksek	Yüksek
İtibar	Çok yüksek	Yüksek
Geliştirici	Linux Vakfı öncülüğünde, Hyperledger Vakfı	R3 konsorsiyumu
Güvenilirlik	Çok yüksek	Yüksek

Sonuç olarak; izin gerektiren özel (private) bir blokzincir tasarımı ve akıllı sözleşme desteğinin mutlaka istenen özellikler olduğu, ölçeklenebilirlik, işlem hızı ve işlem hacminin düşük, sistem güvenliği, mevzuata uyum ve şeffaflığın yüksek önem düzeyinde olduğu, güvenilir ve popüler olması beklenen bir çözüm için en uygun blokzincir platformu Hyperledger Fabric'tir,

Modelin kullanılması ile ulaşılan sonuçlar özet olarak aşağıdaki biçimdedir:

- Blokzincirin temel özellikleri kamu ihale süreci uygulaması için uygundur,
- Sunduğu avantajlar ve güçlü yönleri sürecin iyileştirilebilir alanlarına katkı sağlama potansiyeline sahiptir,
- Kamu ihale süreci için dezavantajlı olabilecek özellikleri zincir dışı veri depolama seçeneği ile giderilebilmektedir,

- Kamu ihale sürecinin blokzincir ile yeniden tasarlanması ile sürecin eski durumundaki proje yöneticisi, heyet başkanı, tekliflerin teslim alınmasından sorumlu personel gibi rollerin bazı fonksiyonları akıllı sözleşme kullanımı ile gerçekleştirilebilecektir,
- Süreçte belirli bir zamana kadar gerçekleştirilmesi gereken faaliyetlerin kontrolleri akıllı sözleşmeler ile gerçekleştirilebilecektir,
- Süreç içerisindeki işlemler her bir kullanıcı için tanımlanmış anahtarlarla gerçekleştirileceğinden ve bu anahtarlar her ihale için yenileneceğinden ihale sürecinin kamuya açık biçimde yayınlanmak istenmesi halinde hem anonimlik hem de şeffaflık sağlanabilecektir,
- Süreçteki belgeler zincir dışında tutulup blokzincirde sadece bu belgelerin hash değerleri tutulacak, böylelikle hem ölçeklenebilirlik hem de gizlilik ve güvenlik sağlanabilecektir,

Kamu ihale sürecinde blokzincir teknolojisinin kullanılabilir olduğu, sürecin yönetişim yapısının blokzincir tasarımına uygun olduğu, blokzincirin bu süreç için gizlilik, güvenlik, erişim kontrolleri ve şeffaflık bakımlarından avantaj sağlayabileceği, blokzincir ile sürecin daha hızlı biçimde işleyebileceği değerlendirilmektedir.

6. SONUÇ VE ÖNERİLER

Her yeni teknoloji sunduğu fırsatlar yanında içerisinde riskler de barındırmaktadır. Son yılların en öne çıkan konularından biri olan blokzincir için de bu durum geçerlidir. Teknolojinin sunduğu fırsatlardan azami düzeyde faydalanmak, risklerini de olabildiğince minimize etmek için çok iyi biçimde anlaşılması, olumlu ve olumsuz tüm tarafları ile ele alınması gerekmektedir. Her yeni teknolojide olduğu gibi, blokzincirde de fırsatları kaçırma güdüsü ile acele karar verme ya da temkinli olma stratejisi ile geç kalma en temel riskler olarak görülmektedir.

Rogers (1983: 246-247) ilk olarak 1962 yılında ortaya attığı İnovasyonun Yayılması Teorisi ile bir fikir ya da ürünün yayılması ve benimsenmesine ilişkin olarak toplumu beş sınıfa ayırmaktadır. Bu sınıflar "yenilikçiler", "erken benimseyenler", "erken çoğunluk", "geç çoğunluk" ve "gecikenler" biçimindedir. Bu teoriye göre popülasyonun %2,5'unu yenilikçiler, %13,5'ini erken benimseyenler, %34'ünü erken çoğunluk, %34'ünü geç çoğunluk, %16'sını da gecikenler oluşturmaktadır. Bu gruplandırma aynı zamanda teknolojinin ilk ortaya çıktığı zaman ile de bağlantılı olup bir zaman serisi üzerinde ilerledikçe yenilikçiler ile gecikenler arasında bir grup içerisinde yer alınmakta, yer alınan zaman ve grup da teknolojinin fırsatlarından yararlanma veya riskleri üstlenme konusunda fayda ya da zararın derecesini ifade etmektedir. Blokzincir teknolojisi için de bu teori geçerlidir. Teknolojinin ilk olarak duyurularak Bitcoin ile uygulanmaya başlandığı dönemden itibaren ilk yıllarda Bitcoin, Ethereum, Ripple gibi platformlar öne çıkmış ve kendilerini kanıtlayarak (riskleri de alarak) en büyük kazanca sahip olmuşlardır. Daha sonra, IBM, Microsoft, Amazon gibi teknoloji devleri bu teknolojiye kayıtsız kalmayarak farklı ürün ve hizmetler ortaya koymuş, erken benimseyenler olarak teknolojinin sunduklarından faydalanmaya çalışmışlardır.

Kamu sektörü genellikle bu tip yeniliklerin kabulü konusunda bireyler ve özel teşebbüslerin arkasından geldiğinden, yeni bir teknolojinin benimsenmesi ve uygulanması konusunda karar sürecini kısaltacak ve kararın uygunluğunu geliştirecek karar destek sistemlerinin kullanılmasının kaçınılmaz olduğu değerlendirilmektedir. Bu bağlamda, blokzincir teknolojisinin herhangi bir kamu hizmeti için kullanımı konusunda aceleci davranarak

kaynakların israf edilmesi ya da geç kalınarak sunduğu avantajlardan faydalanılamaması risklerinin yönetilmesine katkı sağlanması önerilen modelin hedeflerinden biridir.

Blokzincir teknolojisinin bir kamu hizmet sürecinde uygulanması gibi kaynak tahsisi ve dönüşüm gerektiren stratejik bir kararın en doğru biçimde verilebilmesi için konu hakkında detaylı bilgi ve veriye sahip olunması, bu bilgi ve verilerin uygun biçimde analiz edilerek karar için bir destek oluşturulması gerekmektedir. Ancak, stratejik düzeyde karar vericilerden bu detayda bilgiye sahip olmaları, bu bilgiyi edinmek için kayda değer düzeyde zaman harcamaları beklenemez. Bu nedenle, karar vericiler için bu bilgi ve verilerin hazırlanarak gerekli analizlerin yapılmış olması, sonuçların öz ve somut bir biçimde sunulması hem yeniliklere zamanında adapte olabilmek hem de kaynaklar etkin biçimde kullanmak ve riskleri yönetmek için en uygun yaklaşımdır. Önerilen model blokzincir teknolojisinin temel özelliklerini bu bağlamda sistematik bir biçimde toplayarak karar süreci ile ilişkilendirmekte, karar vericiden sadece karara esas kriterlerin önem düzeyleri ile yeni tasarım ile ulaşılmak istenen hedefler beklenmektedir. Özetle, model ile, herhangi bir uzmanlığa sahip olunmadan blokzincirin seçilen bir süreç için uygun olup olmadığı, uygun olması halinde hangi platformun seçilmesi gerektiği ve tasarımın temel özellikleri hakkında bilgi sağlayarak karar verme sürecine yardımcı olunması hedeflenmektedir.

Literatürde, blokzincirin kullanılabilirliğine yönelik bazı çalışmalar bulunmaktadır. Wüst ve Gervais (2018), Birch ve diğerleri (2016), Koens ve Poll (2018), Suichies (2015), Anwar (2018), (Mulligan, 2018) blokzincir teknolojisinin kullanılabilir olup olmadığını gösteren karar modelleri önermişlerdir. Bu karar modelleri blokzincir kullanılabilir mi? sorusuna cevap vermekte, bir kısmı hangi blokzincir tipinin (açık, özel, konsorsiyoum) daha uygun olduğunu da göstermektedir. Ancak bu karar modellerinin hiçbirinde kullanılabilir olması halinde hangi platformun kullanılabileceğine dair bir detay sunulmamıştır.

Six, Herbaut ve Salinesi (2020) blokzincir teknolojisinin seçimine kılavuzluk edecek bir karar destek aracı olarak öne sürdükleri yöntemde birçok blokzincir çözüm alternatifinden hangisinin en uygun olduğu sorusunun cevabını blokzincir yazılımının özellikleri (fikir birliği algoritması, blok boyutu, bloklar arası onay zamanı aralığı gibi) ile yazılımın beklenen kalite kriterlerini birlikte değerlendirerek, Çok Kriterli Karar Verme metotlarından TOPSİS ile sonuca ulaşmaktadır. Bu çalışmada kullanılan nitelik sayısı 15, alternatif sayısı ise dörttür. Kullanılan nitelikler yazılım özellikleri ile sınırlı olup alternatif olarak sadece

Bitcoin, Ethereum, Hyperledger Fabric ve Corda değerlendirilmiştir. Çalışmanın sonuç kısmında gelecekte daha fazla blokzincir alternatifinin kullanılmasının hedeflendiği, niteliklere ilişkin ağırlıklandırma için ise sonucu daha güvenilir hale getirmek için AHP kullanılabileceği belirtilmektedir.

Büyüközkan ve Tüfekçi (2021) yedi teknik, dört teknik olmayan kriter ile beş platform alternatifi için blokzincir platform seçiminde Çok Kriterli Karar Verme metotlarından VIKOR kullanarak bir karar destek sistemi önermektedir. Bu çalışmada alternatiflerin diğer blokzincir platformları ile genişletilebileceği, yeni değerlendirme kriterlerinin ilave edilebileceği ve Çok Kriterli Karar Verme metotlarından diğerlerinin kullanılabileceği belirtilmektedir.

Bu tez çalışmasında önerilen model hem blokzincir kullanımına yönelik karar için gerekli özellikleri (blokzincir özellikleri ile blokzincir platformlarının özellikleri) içeren bir bilgi tabanının sistematik bir biçimde oluşturulmasını, toplanan bilgilere dayalı kuralların geliştirilmesini, kullanıcı ya da karar vericiden süreç ve öncelikler hakkında sistematik bir biçimde girdi sağlanmasını, bu girdiler doğrultusunda kriterlerin önceliklendirilerek her bir platform alternatifinin birbiri ile ikili karşılaştırmaları yapılarak değerlendirilmesini içermektedir.

Önerilen model, yatay ve dikey olarak genişletilebilir bir yapıdadır. Yatay genişleme platform alternatifi ilavesi ile gerçekleştirilebilmektedir. Hazırlanmış olan blokzincir platformu özellik tablosu şablonu kullanılarak hâlihazırda önerilen 14 platforma ek olarak modele yeni platform tanımlaması yapılabilmektedir. Dikey genişleme ise mevcut platform özellik tablosuna ve modelde kullanılan diğer listelere (blokzincir avantajları, kısıtlılıkları, kullanım alanları gibi) yeni özellikler ilave edilerek gerçekleştirilebilecektir. Bu genişletilebilir yapı platform özelliklerinin listelenmesi için hazırlanmış olan standart form, özellik listeleri, kriterlerin belirlenmesi ve önceliklendirilmesi için kullanılan MoSCoW nitelik tablosu, bu tabloya uyumlu biçimde hazırlanmış olan Süreç Bilgi Toplama Formu gibi liste ve şablonlarla sağlanmaktadır. Belirtilen şablonlara uygun biçimde eklenecek kriter ya da platform alternatifinin modelin işleyişine bir etkisi bulunmamaktadır.

Model kapsamında önerilen çözümün doğrulanması ya da güvenilirliğinin ölçülmesi benzer ya da kabul gören, karşılaştırma yapma olanağı sunan bir seçim metodunun olmaması, model

ile gerçekleştirilen işlemlerin süreç özellikleri, kullanıcı tercihleri ve önceliklerine göre farklılık göstermesi nedeniyle standart bir yapısının olmaması, bu nedenle, aynı süreç için farklı kurumlarda bile kullanıcı önceliklerine göre farklı sonuç elde edilebilmesinin mümkün ve beklenen durum olması nedenleriyle oldukça güçtür. Bununla birlikte, modelin geçerliliği, hâlihazırda gerçek dünya uygulaması bulunan uygulamalarda kullanılan platformlar ile elde edilen sonucun karşılaştırılması ya da birden çok blokzincir uzmanının görüşüne başvurulması biçiminde iki yol ile ölçülebilir. Model önerisi işlem adımlarının kamu ihale süreci için uygulanması sonucunda elde edilen sonucun karşılaştırılması için dünya devletlerinden blokzincirin ihale sürecine uygulanma örnekleri literatür tarama ile araştırılmıştır. Nanayakkara, Rodrigo, Perera, Weerasuriya ve Hijazi (2021); Bustamante ve diğerleri (2022); Mohite ve Acharya (2018) ve Logith, Nitish, Raghul ve Tamilarasan (2022) tedarik sürecinde blokzincir kullanımında Hyperledger platformunun kullanımına ilişkin öneri ve örnekler sunmaktadır. Buna göre, ihale sürecinde blokzincir kullanımı için genel olarak tercih edilen platform alternatifinin model çıktısına benzer biçimde Hyperledger olduğu görülmektedir.

Önerilen modelde Çok Kriterli Karar Verme metodu olarak Analitik Hiyerarşi Prosesi kullanılmıştır. Kriter ve alternatif sayısının çok fazla olması halinde işlemleri kolaylaştırmak adına Ağırlıklı Toplam Metodu gibi daha basit modeller kullanılabileceği gibi verilecek kararın niteliği dikkate alınarak bulanık AHP gibi daha hassas ve karmaşık metotlar da kullanılabilir.

Bu tez çalışmasında önerilen model ile ilk aşamada blokzincirin seçilen süreç için uygun olup olmadığı kararının sunulması, daha sonra kullanıcı ya da karar verici tarafından belirlenen kriterler ve önceliklere göre herhangi bir detaylı hesaplama işlemi gerçekleştirilmeden uygun olmayan alternatiflerin doğrudan elenmesi, son aşamada da kalan alternatiflerin birbirleri ile karşılaştırılıp puanlanarak uygunluklarına göre sıralanması karar sürecinin kısaltılmasına, karar aşamasında hem teknik özelliklerin hem de kullanıcı tercihlerinin bir arada değerlendirilerek daha etkin bir karar verilmesine, değerlendirme sonucuna göre önerilen sistemin tasarımına ilişkin çıktılar üreterek de beklenen çözümün ilgili taraflara açık ve anlaşılır biçimde aktarılmasına katkıda bulunduğu değerlendirilmektedir.

Önerilen model çok sayıda işlem adımı ve karar aşamalarını, dış bilgi girişini, işlemlerin gerçekleştirilmesi için gereken kural ve listeleri içermekte olup bu kurallar, listeler, kullanıcı öncelikleri ve seçim alternatifleri arasındaki bağlantıların manuel olarak yönetilmesi mümkündür. Ancak, bu biçimde kullanımı zaman alıcıdır ve çok sayıda alt detay ve işlem adımı içerdiğinden hataya açıktır. Öte yandan, Çok Kriterli Karar Verme metodu olarak kullanılan Analtik Hiyerarşi Prosesi de kriter ve alterntif sayısı artıkça karmaşıklaşan ve adedi artan hesaplama işlemlerine sahiptir. Bu hesaplamaların, tutarlılık analizlerinin ve sonuçların sunumunun daha sistematik, hızlı ve kullanışlı hale getirilebilmesi bakımından bir web arayüzü ile kullanılabilecek biçimde yazılımsal olarak tasarlanması önerilen modelin etkinliğini ve kullanım kolaylığını artıracaktır.

Önerilen model, karar verme aşaması dışında, blokzincir teknolojisini bir kamu hizmet sürecinde kullanmayı hedefleyen kamu kurumlarının gerek kendi kabiliyetleri ile uygulama geliştirmeleri, gerekse hizmet alımı ile blokzinciri kullanmaları halinde gereksinim duyacakları proje tanımlama dokümanı ya da ihale şartnamesinin hazırlanması aşamalarında da kullanılabilirdir.

Blokzincir teknolojisi hâlâ gelişiminin ilk aşamalarındadır ve dijital dönüşüm potansiyeli hâlâ büyük ölçüde kullanılamamaktadır. Bu bağlamda, önerilen modelin kamu hizmetlerinin dijital dönüşümüne katkı sağlayacak etkin, hızlı ve uygun kararların verilmesi konusunda fayda sağlaması beklenmektedir.

KAYNAKLAR

Abugaliyeva, M. (2018, 3 20). *Kazakh National Bank issues short-term notes through Invest Online*. 1 15, 2021 tarihinde The Astana Times web sitesi: http://web.archive.org/web/20210115123534/https://astanatimes.com/2018/03/kazakh-national-bank-issues-short-term-notes-through-invest-online/ adresinden alındı.

Ahmad, T. (2018). *Regulation of Cryptocurrency in Selected Jurisdictions, Canada.* Washington: The Law Library of Congress USA.

Allessie, D., Sobolewski, M., & Vaccari, L. (2019). *Blockchain for digital government.* Luxembourg: Publications Office of the European Union.

Allison, I. (2017, 8 23). *Ethereum identity system uPort working with Brazil's Ministry of Planning*. 1 16, 2021 tarihinde International Business Times web sitesi: http://web.archive.org/web/20210116131640/https://www.ibtimes.co.uk/ethereum-identity-system-uport-working-brazils-ministry-planning-1636253 adresinden alındı

Almanya Ekonomik İşler ve Enerji Bakanlığı (BMWi). (2019). *Blockchain Strategy of the Federal Government.* Berlin: BMWi.

Almanya Maliye Bakanlığı. (2019, 9 18). *Financial Markets: German government adopts blockchain strategy*. 1 15, 2021 tarihinde Federal Ministry of Finance web sitesi: http://web.archive.org/web/20210115110611/https://www.bundesfinanzministerium.de/Content/EN/Standardartikel/Topics/Financial_markets/Articles/2019-09-18-Blockchain.html adresinden alındı.

Alonso, J. A., & Lamata, M. (2006). Consistency In The Analytic Hierarchy Process: A New Approach. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, 14*(4), 445-459.

Anwar, H. (2018, 10 4). *Do You Need a Blockchain? The Ultimate Blockchain Decision Tree*. 101 Blockchains web sitesi: http://web.archive.org/web/20201112194717/https://101blockchains.com/do-you-need-a-blockchain/ adresinden alındı.

ASTRI. (2016, 11 11). Whitepaper On Distributed Ledger Technology. *Whitepaper - Hong Kong Monetary Authority* . Hong Kong: Hong Kong Monetary Authority.

Atzei, N., Bartoletti, M., & Cimoli, T. (2017). A Survey of Attacks on Ethereum Smart Contracts (SoK). *Proceedings of the 6th International Conference on Principles of Security and Trust* (s. 164-186). Berlin: Springer.

Austrian Federal Computing Center (BRZ). (2020, 1 29). *Building bridges: e-participation combined with virtual reality*. 1 14, 2021 tarihinde Avusturya Federal Bilgi İşlem Merkezi web sitesi: http://web.archive.org/web/20210114171706/https://www.brz.gv.at/en/how_we_operate/e-participation-combined-with-virtual-reality-.html adresinden alındı.

Avrupa Komisyonu. (2017, 7 21). Tender Specifications. *European Blockchain Observatory and Forum Setting-up and Running a European Expertise Hub on Blockchain and Distributed Ledger Technologies*. Brüksel, Belçika: Avrupa Komisyonu.

Avrupa Komisyonu. (2018, 2 1). European Commission - Press release. *European Commission launches the EU Blockchain Observatory and Forum*. Brüksel, Belçika: Avrupa Komisyonu.

Avrupa Komisyonu. (2019). *Digital Government Factsheet 2019, Latvia.* Brüksel: Avrupa Komisyonu.

Avusturya Ticaret Odası. (2019). *Blokzincir hizmet veri sertifikası*. 1 14, 2021 tarihinde Avusturya Ticaret Odası Web sitesi: https://web.archive.org/web/20201026024955/https://www.wko.at/service/innovation-technologie-digitalisierung/blockchain.html adresinden alındı.

Awataguchi, T., & Nagase, T. (2020). Japan. J. N. Dewey içinde, *Blockchain & Cryptocurrency Regulation* (s. 414). London: Global Legal Group Ltd.

Bacchi, U. (2017, 11 15). *Moldova eyes blockchain to end child trafficking*. 11 8, 2020 tarihinde Business & Financial News, U.S. & International Breaking News | Reuters: http://web.archive.org/web/20201108195655/https://www.reuters.com/article/us-moldova-blockchain-child-trafficking/moldova-eyes-blockchain-to-end-child-trafficking-idUSKBN1DF2GQ adresinden alındı.

Back, A. (1997, 3 28). *Hashcash duyuru sayfası*. 2 14, 2021 tarihinde Hashcash.org web sitesi: http://web.archive.org/web/20210125175806/http://www.hashcash.org/papers/announce.txt adresinden alındı.

Back, A. (2002). Hashcash - A Denial of Service Counter-Measure. *Computer Science*, 1-10.

BAE Hükumeti. (2020, 7 12). *Blockchain in the UAE government*. 10 12, 2020 tarihinde BAE Hükumeti resmi sayfası: http://web.archive.org/web/20210115084857/https://u.ae/en/about-the-uae/digital-uae/blockchain-in-the-uae-government adresinden alındı.

BAE Hükumeti. (2020, 1 16). *Emirates Blockchain Strategy 2021*. BAE Federal Hükumeti web sitesi: http://web.archive.org/web/20210115084230/https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/federal-governments-strategies-and-plans/emirates-blockchain-strategy-2021 adresinden alındı.

Bahrain Fintech Bay. (2017, 11 6). *Largest Dedicated Fintech Hub in Mena Region to Launch in Bahrain*. 1 15, 2021 tarihinde Bahrain Fintech Bay web sitesi: http://web.archive.org/web/20210115210737/https://www.bahrainfintechbay.com/single-post/2017/11/06/largest-dedicated-fintech-hub-in-mena-region-to-launch-in-bahrain adresinden alındı.

Baliga, A. (2020). *Understanding Blockchain Consensus Models.* Santa Clara, CA: Persistent Systems Ltd.

Bangkok Post. (2020, 10 28). *Cambodia officially launches digital currency backed by central bank*. 1 16, 2021 tarihinde Bangkok Post web sitesi: https://www.bangkokpost.com/tech/2009915/cambodia-officially-launches-digital-currency-backed-by-central-bank adresinden alındı.

Bank Frick. (2019, 2 20). *Bank Frick is establishing The DLT Markets AG to provide institutional investors with professional access to digital assets*. 11 16, 2020 tarihinde Bank Frick Web sitesi: http://web.archive.org/web/20201116202414/https://www.bankfrick.li/en/about-bank-frick/media/bank-frick-is-establishing-the-dlt-markets-ag-to-provide-institutional-investors-with-professional-access-to-digital-assets adresinden alındı.

Bank of Lithuania. (2020, 3 23). *LBChain*. Bank of Lithuania web sitesi: https://web.archive.org/web/20210114204536/https://www.lb.lt/en/lbchain adresinden alındı.

Bankacılık Düzenleme ve Denetleme Kurumu (BDDK). (2013, 11 25). Basın Açıklaması. *BDDK Duyuruları* . İstanbul: BDDK.

Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., & Danezis, G. (2017). SoK: Consensus in the Age of Blockchains. *arXiv:1711.03936* , 1-17.

Bartlett, J. (2016). *Dark Net İnternetin Yeraltı Dünyası.* İstanbul: Timaş Yayınları.

Bayer, D., Haber, S., & Stornetta, W. S. (1993). Improving the Efficiency and Reliability of Digital Time-Stamping. *Sequences II: Methods in Communication, Security and Computer Science,* (s. 329-334). New York: Springer.

Belarus Blockchain Association. (tarih yok). *Home: Blockchain Belarus*. 1 15, 2021 tarihinde Belarus Blockchain Association web sitesi: http://web.archive.org/web/20210115212428/http://blockchainbelarus.by/?q=en adresinden alındı.

Belton, V., & Gear, T. (1983). On a short-coming of Saaty's method of analytic hierarchies. *Omega, 11*(3), 228-230.

Beretta, J. (2019). UAE. J. Dewey içinde, *Blockchain & Cryptocurrency Regulation* (s. 459). London: Global Legal Group Ltd.

BERNAMA Media Relations and Event Management. (2019, 12 12). *Press Releases: BERNAMA Media Relations and Event Management (MREM)*. 1 16, 2021 tarihinde BERNAMA Media Relations and Event Management web sitesi: http://web.archive.org/web/20210116122054/http://mrem.bernama.com/viewsm.php?idm=36396 adresinden alındı.

Berryhill, J., Bourgery, T., & Hanson, A. (2018). *Blockchains Unchained: Blockchain Technology and its Use in the Public Sector, OECD Working Papers on Public Governance, No. 28.* Paris: OECD Publishing. http://dx.doi.org/10.1787/3c32c429-en adresinden alındı.

Bhunia, P. (2018, 1 4). 3 24, 2018 tarihinde Opengovasia : https://www.opengovasia.com/articles/how-the-dutch-government-is-exploring-

potential-uses-of-blockchain-through-many-concurrent-pilot-projects adresinden alındı.

BigchainDB GmbH. (2018, 5). BigchainDB 2.0 The Blockchain Database. *BigchainDB 2.0 Whitepaper*. Berlin, Germany: BigchainDB GmbH.

Bilgi Teknolojileri ve İletişim Kurumu. (2020). *Kripto Para Araştırma Raporu.* Ankara: Bilgi Teknolojileri ve İletişim Kurumu.

Birch, D., Brown, R. G., & Parulava, S. (2016). Towards ambient accountability in financial services: Shared ledgers, translucent transactions and the technological legacy of the great financial crisis. *Journal of Payments Strategy & Systems, 10*(2), 118-131.

Birleşmiş Milletler. (2020). *E-Government Survey 2020.* New York: Birleşmiş Milletler.

Birleşmiş Milletler. (2022). *E-Government Survey 2022.* New York: Birleşmiş Milletler.

Bitcoin.org. (2014). *History of Bitcoin*. 2 18, 2021 tarihinde Bitcoin.org web sitesi: http://web.archive.org/web/20210218085400/http://historyofbitcoin.org/ adresinden alındı

Bitfury. (2017, 4 13). Ukrainian Government Partners with The Bitfury Group to Create First Full-Scale Blockchain eGovernance Program for Ukraine. *Press Release*. Kyiv, Ukraine: Bitfury.

Bitfury. (tarih yok). *Exonum: Rebuilding citizen trust in government e-auctions*. 1 16, 2021 tarihinde Bitfury Exonum web sitesi: http://web.archive.org/web/20210116133744/https://exonum.com/story-ukraine adresinden alındı

Blacklock, J., & Lei, S. (2020). China. J. N. Dewey içinde, *Blockchain & Cryptocurrency Regulation* (s. 316). London: Global Legal Group Ltd.

Blockchain Federal Argentina (BFA). (2018). *What is BFA?* 1 15, 2021 tarihinde Blockchain Federal Argentina web sitesi: http://web.archive.org/web/20210115131101/https://bfa.ar/en/bfa/what-bfa adresinden alındı

Blockchain Israel. (2017, 1 30). *Mission: Blockchain Israel*. 1 15, 2021 tarihinde Blockchain Israel web sitesi: http://web.archive.org/web/20210115124130/http://blockchainisrael.org/mission adresinden alındı

Blockchain Slovakia. (2017). *About us: Blockchain Slovakia*. 1 16, 2021 tarihinde Blockchain Slovakia web sitesi: http://web.archive.org/web/20180317060704/http://blockchainslovakia.sk/en/onas/ adresinden alındı

Blokzincir Araştırma Laboratuvarı. (2017). *BZLab*. 10 29, 2022 tarihinde TÜBİTAK BİLGEM: http://web.archive.org/web/20221029131816/https://blokzincir.bilgem.tubitak.gov.tr/hakkimizda/ adresinden alındı

Boğaziçi Üniversitesi Bilgisayar Mühendisliği Bölümü. (2022). *Undergraduate Courses | CmpE WEB*. 10 29, 2022 tarihinde CmpE WEB: https://web.archive.org/web/20221029133334/https://www.cmpe.boun.edu.tr/courses/undergraduate adresinden alındı

Boğaziçi Üniversitesi İşletme Bilişim Sistemleri Programı. (2020). *Curriculum - Business Information Systems*. 11 9, 2020 tarihinde Business Information Systems - Master of Arts Program: http://web.archive.org/web/20200428093512/http://bis.boun.edu.tr/en/curriculum/ adresinden alındı

Boring, N. (2018). *Regulation of Cryptocurrency in Selected Jurisdictions, France.* Washington: The Law Library of Congress USA.

Boucher, P., Nascimento, S., & Kritikos, M. (2017). *How blockchain technology could change our lives.* Brussels: Scientific Foresight Unit (STOA), European Parliament.

Brainard, L. (2020, 8 13). An Update on Digital Currencies. *Basın Bildirisi*. San Francisco: Board of Governors of the Federal Reserve System.

Brainbot Technologies. (2016). *HydraChain*. 4 15, 2021 tarihinde HydraChain GitHub Repository: http://web.archive.org/web/20201108141627/https://github.com/HydraChain/hydrachain adresinden alındı

Brender, N., Gauthier, M., Morin, J.-H., & Salihi, A. (2018). *The Potential Impact of Blockchain Technology on Audit Practice.* Geneva: University of Applied Sciences and Arts Western Switzerland.

British Columbia Eyaleti. (2020, 12 16). *Verifiable Organizations Network: github*. 1 15, 2021 tarihinde Github web sitesi: http://web.archive.org/web/20210115120728/https://github.com/bcgov/von adresinden alındı

Buchanan, K. (2018). *Regulation of Cryptocurrency in Selected Jurisdictions, Australia.* Washington: The Law Library of Congress USA.

Burbidge, M. (2016, 10 17). *ITWeb: SA banks, Strate set up blockchain network*. 1 16, 2021 tarihinde ITWeb web sitesi: http://web.archive.org/web/20210116142630/https://www.itweb.co.za/content/nG98YdMLElDqX2PD adresinden alındı

Bustamante, P., Cai, M., Gomez, M., Harris, C., Krishnamurthy, P., Law, W., . . . Weiss, M. (2022). Government by Code? Blockchain Applications to Public Sector Governance. *Front. Blockchain, 5*(869665).

Buterin, V. (2013). A Next Generation Smart Contract & Decentralized Application Platform. *Ethereum White Paper*.

Buterin, V. (2013, 7 31). *Bitcoin Is Not Quantum-Safe, And How We Can Fix It When Needed*. 2 16, 2021 tarihinde Bitcoinmagazine web sitesi:

http://web.archive.org/web/20210111105112/https://bitcoinmagazine.com/articles/bitcoin-is-not-quantum-safe-and-how-we-can-fix-1375242150 adresinden alındı

Buterin, V. (2014, 5 6). *DAOs, DACs, DAs and More: An Incomplete Terminology Guide*. 11 9, 2020 tarihinde Ethereum Blog Web sitesi: http://web.archive.org/web/20201109172425/https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/ adresinden alındı

Büyüközkan, G., & Tüfekçi, G. (2021). A decision-making framework for evaluating appropriate business blockchain platforms using multiple preference formats and VIKOR. *Information Sciences*(571), 337-357.

C Minds. (2018, 2). *RUCAM: Blockchain For Better Public Services*. 1 16, 2021 tarihinde C Minds web sitesi: http://web.archive.org/web/20210116150227/https://www.cminds.co/blockchain adresinden alındı

Castro, M., & Liskov, B. (2002). Practical Byzantine Fault Tolerance and Proactive Recovery. *ACM Transactions on Computer Systems*, 398-461.

Chang, D. (2017, 6 23). *Haberler: Çin Devlet Konseyi*. 1 16, 2021 tarihinde Çin Devlet Konseyi web sitesi: http://web.archive.org/web/20200206072322/http://www.gov.cn/xinwen/2017-06/23/content_5204956.htm adresinden alındı

Chartered Accountants Australia and New Zealand. (2017). *The Future of Blockchain: Applications and Implications of Distributed Ledger Technology.* Sydney: Chartered Accountants Australia and New Zealand.

Chaum, D. (1981). Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms. *Communications of the ACM, 24*(2), 84-88.

Chaum, D. (1982). Computer Systems Established, Maintained and Trusted by Mutually Suspicious Groups. *Dissertation of Doctor of Philosophy*. Berkeley: University of Californa.

Chaum, D. (1983). Blind Signatures for Untraceable Payments. D. Chaum, R. L. Rivest, & A. T. Sherman içinde, *Advances in Cryptology* (s. 199-203). Boston: Springer.

Chaum, D. (1994, 5 27). *World's first electronic cash payment over computer networks*. 2 14, 2021 tarihinde DigiCash Project Page: http://web.archive.org/web/20200927103914/https://www.chaum.com/ecash/articles/1994/05-27-94%20-%20World_s%20first%20electronic%20cash%20payment%20over%20computer%20networks.pdf adresinden alındı

Chavez-Dreyfuss, G. (2015, 5 15). *Honduras to build land title registry using bitcoin technology*. 1 16, 2021 tarihinde Reuters web sitesi: http://web.archive.org/web/20210116143429/https://www.reuters.com/article/usa-honduras-technology-idINKBN0O01V720150515?edition-redirect=in adresinden alındı

Chitra, T., Quaintance, M., Haber, S., & Martino, W. (2019). Agent-Based Simulations of Blockchain protocols illustrated via Kadena's Chainweb. arXiv:1904.12924v1.

Ciambella, F., Chong, E.-L., & Lin, Y. (2019). Singapore. J. Dewey içinde, *Blockchain & Cryptocurrency Regulation* (s. 420). London: Global Legal Group Ltd.

CoinMarketCap. (2019, 4 1). *Coin Market Capitalization*. 3 22, 2019 tarihinde https://coinmarketcap.com/coins/views/market-cap-by-total-supply/ adresinden alındı

CoinMarketCap. (2022, 10 26). *Cryptocurrency Prices, Charts and Market Capitalizations*. 11 30, 2020 tarihinde CoinMarketCap Web sitesi: https://web.archive.org/web/20221026122632/https://coinmarketcap.com/ adresinden alındı

Commonwealth of Australia, Department of the Prime Minister and Cabinet. (2015). *National Innovation and Science Agenda Report.* Commonwealth of Australia, Department of the Prime Minister and Cabinet.

Czech Republic Blockchain Republic. (tarih yok). *Home: Blockchain Republic*. 1 15, 2021 tarihinde Blockchain Republic web sitesi: http://web.archive.org/web/20210115211617/https://www.blockchainrepublic.cz/english adresinden alındı.

Çarkacıoğlu, D. A. (2016). *Kripto Para Bitcoin.* Ankara: Sermaye Piyasası Kurulu (SPK).

Dai, J. (2017, 10). A Dissertation for the degree of Doctor of Philosophy. *Three Essays on Audit Technology: Audit 4.0, Blockchain, and Audit App*. New Jersey: The State University of New Jersey.

Dai, W. (1998). *b-money*. weidai.com web sitesi: http://web.archive.org/web/20210106143307/http://www.weidai.com/bmoney.txt adresinden alındı.

Davis, S. (2019, 10 8). *Burrow – The Boring Blockchain*. 2 28, 2021 tarihinde Hyperledger web sitesi: http://web.archive.org/web/20210228135757/https://www.hyperledger.org/blog/2019/10/08/burrow-the-boring-blockchain adresinden alındı.

Davis, S., Maxson, S., & Moyle, A. (2020, 10 23). *Blockchain Laws and Regulations, United Kingdom*. 10 29, 2020 tarihinde Global Legal Insights web sitesi: http://web.archive.org/web/20201029093718/https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/united-kingdom adresinden alındı

Davradakis, E., & Santos, R. (2019). Blockchain, FinTechs and their relevance for international financial institutions. *European Investment Bank (EIB) Working Papers No. 2019/01*. Luxembourg: EIB.

DECODE. (tarih yok). *DECODE Project: Have more questions?* 1 16, 2021 tarihinde DECODE web sitesi: http://web.archive.org/web/20210116135248/https://decodeproject.eu/have-more-questions adresinden alındı

Deng, H. (1999). Multicriteria analysis with fuzzy pairwise comparison. *International Journal of Approximate Reasoning*(21), 215-231.

Dewey, J. N. (2019). USA. J. N. Dewey içinde, *Blockchain & Cryptocurrency Regulation* (s. 479). London: Global Legal Group Ltd.

Dewey, J. N. (2020, 10 23). *Blockchain Laws and Regulations, USA*. 10 29, 2020 tarihinde Global Legal Insights web sitesi: http://web.archive.org/web/20201029122818/https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/usa adresinden alındı

Diffie, W., & Hellman, M. E. (1976). New Directions in Cryptography. *IEEE Transactions on Information Theory, IT-22*(6), 644-654.

Diffie, W., & Hellman, M. E. (1979). Privacy and authentication: An introduction to cryptography. *Proceedings of the IEEE, 67*(3), 397-427.

Dijital Dönüşüm Ofisi Başkanlığı. (2020, 10 7). *Hakkımızda: turkiye.gov.tr*. 8 4, 2021 tarihinde e-Devlet Kapısı Devletin Kısayolu: http://web.archive.org/web/20210408203857/https://www.turkiye.gov.tr/bilgilendirme?konu=siteHakkinda adresinden alındı

Dinh, T. T., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018, 7 1). Untangling Blockchain: A Data Processing View of Blockchain Systems. *IEEE Transactions on Knowledge and Data Engineering*, 1366-1385.

Diwakar, A. (2022, 02 23). *Decentralised Finance (DeFi) explained*. 10 27, 2022 tarihinde TRT World: http://web.archive.org/web/20221026211826/https://www.trtworld.com/magazine/decentralised-finance-defi-explained-55051 adresinden alındı

Donna, M., & Di Maria, L. C. (2020, 10 23). *Blockchain Laws and Regulations, Italy*. 10 26, 2020 tarihinde Global Legal Insights web sitesi: https://web.archive.org/web/20201026130719/https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/italy adresinden alındı

Donna, M., & Di Maria, L. C. (2020, 10 23). *Blockchain Laws and Regulations, Italy*. 1 15, 2021 tarihinde Global Legal Insights web sitesi: http://web.archive.org/web/20210115204334/https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/italy adresinden alındı

Dubai Future Foundation. (2016, 2 16). *Insights: Dubai Future Foundation*. 1 15, 2021 tarihinde Dubai Future Foundation web sitesi: http://web.archive.org/web/20210115091227/https://www.dubaifuture.ae/insights/dubai-museum-of-the-future-foundation-announces-launch-of-global-blockchain-council/ adresinden alındı

Dubai Land Department. (2017, 10 7). *News - Media: Dubai Land Department*. 1 15, 2021 tarihinde Dubai Land Department web sitesi: http://web.archive.org/web/20210115092722/https://dubailand.gov.ae/en/news-media/dubai-land-department-achieves-a-technical-milestone-with-the-adoption-of-

blockchain-technology-in-cooperation-with-smart-dubai-and-other-partners/ adresinden alındı

Dubois, D., Lang, J., & Prade, H. (1991). Fuzzy Sets in Approximate Reasoning, Part 2: Logical Approaches. C. V. Negoita, L. A. Zadeh, & H. J. Zimmermann içinde, *Fuzzy Sets and Systems* (s. 203-244). NJ: Elsevier Science Publishers B.V. (North-Holland).

Dünya Bankası. (2019, Ekim). ID4D Practitioner's Guide. *Dünya Bankası Yayınları*. Washington, Amerika Birleşik Devletleri: World Bank Publications.

Dwork, C., & Naor, M. (1993). Pricing via Processing or Combatting Junk Mail. *Advances in Cryptology — CRYPTO'92* (s. 139-147). Berlin: Springer.

Dyer, J. S. (1990). Remarks on the Analytic Hierarchy Prtocess. *Management Science, 36*(3), 249-258.

Ebert, J. (2019). *MIT Solve: A toolkit for gathering and documenting valid consent*. 1 16, 2021 tarihinde Massachusetts Institute of Technology (MIT) Solve initiative web sitesi: http://web.archive.org/web/20210116142241/https://solve.mit.edu/challenges/id4d-mission-billion/solutions/5889 adresinden alındı

EconoTimes. (2016, 1 11). *Tunisia To Replace eDinar With Blockchain-Based Currency*. 1 16, 2021 tarihinde EconoTimes web sitesi: http://web.archive.org/web/20210116151740/http://www.econotimes.com/Tunisia-To-Replace-eDinar-With-Blockchain-Based-Currency-140836 adresinden alındı

e-Estonia Briefing Centre. (tarih yok). *KSI blockchain sayfası*. 1 14, 2021 tarihinde e-Estonia web sayfası: https://web.archive.org/web/20210114155919/https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/ adresinden alındı

Emrouznejad, A., & Ho, W. (2018). Analytic Hierarchy Process and Fuzzy Set Theory. A. Emrouznejad, & W. Ho içinde, *Fuzzy Analytic Hierarchy Process* (s. 1-11). Boca Raton, FL: CRC Press Taylor & Francis Group.

Ethereum.org. (2022, 9 27). *Blocks*. 10 27, 2022 tarihinde Ethereum web sitesi: https://web.archive.org/web/20221027200817/https://ethereum.org/en/developers/docs/blocks/ adresinden alındı

EU Blockchain Observatory and Forum. (2020, 5 29). *Reflections: Reviewing the first two years of the EU Blockchain Observatory*. EU Blockchain Observatory and Forum Web sitesi: http://web.archive.org/web/20201115124924/https://www.eublockchainforum.eu/news/reflections-reviewing-first-two-years-eu-blockchain-observatory adresinden alındı

Falzon, M., & Valenzia, A. (2019). Malta. J. Dewey içinde, *Blockchain & Cryptocurrency Regulation* (s. 378). London: Global Legal Group Ltd.

Federal Antimonopoly Service of the Russian Federation. (2016, 10 17). *Press-Center: Federal Antimonopoly Service of the Russian Federation*. 1 15, 2021 tarihinde Federal Antimonopoly Service of the Russian Federation web sitesi:

http://web.archive.org/web/20210115163859/http://en.fas.gov.ru/press-center/news/detail.html?id=47456 adresinden alındı

Figueira, J., Mousseau, V., & Roy, B. (2005). Electre Methods. S. Greco içinde, *Multiple Criteria Decision Analysis: State of the Art Surveys* (s. 133-153). New York: Springer.

Finck, M. (2018). Blockchains and Data Protection in the European Union. *European Data Protection Law Review, 4*(1), 17-35. doi:https://doi.org/10.21552/edpl/2018/1/6

Finney, H. (2004, 8 15). *RPOW - Reusable Proofs of Work*. 2 16, 2021 tarihinde Nakamoto Institute web sitesi: http://web.archive.org/web/20201112001948/https://nakamotoinstitute.org/rpow/ adresinden alındı

Forbes, D. (2021, 2 24). *Consensus*. 4 21, 2021 tarihinde Substrate Developer Hub Knowledge Base: http://web.archive.org/web/20210421213310/https://substrate.dev/docs/en/knowledgebase/advanced/consensus adresinden alındı

France Strategie. (2017, 5 9). Information Presse - Les enjeux des blockchains. *Les enjeux des blockchains*. Paris, France: France Strategie.

Fransham, J. (2018, 7 9). *What is Substrate?* 4 21, 2021 tarihinde Parity web sitesi: http://web.archive.org/web/20210421204341/https://www.parity.io/what-is-substrate/ adresinden alındı

Fridgen, G., Guggenmos, F., Lockl, J., Rieger, A., Schweizer, A., & Urbach, N. (2018). Developing an Evaluation Framework for Blockchain in the Public Sector: The Example of the German Asylum Process. *Developing an Evaluation Framework for Blockchain in the Public Sector: The Example of the German Asylum Process.*

Gesley, J. (2018). *Regulation of Cryptocurrency in Selected Jurisdictions, Switzerland.* Washington: The Law Library of Congress USA.

Github.com. (2021, 2 24). *Bitcoin Github sayfası*. 2 27, 2021 tarihinde Github web sitesi: https://github.com/bitcoin/bitcoin adresinden alındı

GovChain. (2019). *Bahrain - GovChain*. 1 15, 2021 tarihinde GovChain web sitesi: http://web.archive.org/web/20210115210103/https://govchain.world/bahrain/ adresinden alındı

GovChain. (2019). *China - GovChain*. 1 16, 2021 tarihinde GovChain web sitesi: http://web.archive.org/web/20210116120734/https://govchain.world/china/ adresinden alındı

Grant, S., Lim, K., & Peters, M. (2020). Canada. J. N. Dewey içinde, *Blockchain & Cryptocurrency Regulation* (s. 294). London: Global Legal Group Ltd.

Greenspan, G. (2015). MultiChain Private Blockchain. *White Paper*. Coin Sciences Ltd.

Groenfeldt, T. (2017, 6 28). *7 European Banks Form Blockchain Consortium For SMEs*. 1 16, 2021 tarihinde Forbes:

http://web.archive.org/web/20210116140453/https://www.forbes.com/sites/tomgroenfeldt/2017/06/28/7-european-banks-form-blockchain-consortium-for-smes/ adresinden alındı

Güven, V., & Şahinöz, E. (2018). *Blokzincir, Kripto Paralar, Bitcoin.* İstanbul: Kronik Kitap.

Haber, S., & Stornetta , W. S. (1991). How to time-stamp a digital document. *Journal of Cryptology, 3*, 99-111.

Hacettepe Üniversitesi. (2022). *Hacettepe Üniversitesi Bilgisayar Mühendisliği Bölümü*. 10 29, 2022 tarihinde Hacettepe Üniversitesi web sitesi: http://web.archive.org/web/20221019014706/https://www.cs.hacettepe.edu.tr/ adresinden alındı

Haeberli, D., Oesterhelt, S., & Wherlock, A. (2020). Switzerland. J. N. Dewey içinde, *Blockchain & Cryptocurrency Regulation* (s. 524). London: Global Legal Group Ltd.

Haller, N. M. (1994). The S/Key One-Time Password System. *Proceedings of the Symposium on Network & Distributed Systems Security, Internet Society.* San Diego, CA.

Hämäläinen, R. P., & Seppäläinen, T. O. (1986). The analytic network process in energy policy planning. *Socio-Economic Planning Sciences, 20*(6), 399-405.

Hayat , M., & Winkler, H. (2022). An Analytic Hierarchy Process for Selection of Blockchain-Based Platform for Product Lifecycle Management. Sustainability, 14(21), 13703.

Hazine ve Maliye Bakanlığı ve Strateji ve Bütçe Başkanlığı. (2020, 9 29). Orta Vadeli Program (2021-2023). *OVP*. Ankara: T.C. Cumhurbaşkanlığı.

Hearn, M., & Brown, R. G. (2019, 8 20). Corda: A distributed ledger. *Corda Whitepaper*. R3.

Hileman, G., & Rauchs, M. (2017). *Global Blockchain Benchmarking Study.* Cambridge: Cambridge Centre for Alternative Finance.

Hill, F., & Foster, B. (2019, 9 30). Letter to Fed Chairman. *Congress of The United States*. Washington: Congress of The United States.

Ho, W. (2008). Integrated analytic hierarchy process and its applications – A literature review. *European Journal of Operational Research*(186), 211–228.

Hong Kong Legislative Council. (2017, 4 18). Legislative Council Panel on Financial Affairs, Development of Financial Technologies . *Discussion Paper*. Hong Kong: Hong Kong Legislative Council.

Houben, R., & Snyers, A. (2020). *Crypto-assets – Key developments, regulatory concerns and responses.* Luxembourg: European Union.

Hughes, E. (1993, 3 9). *A Cypherpunk's Manifesto*. 2 14, 2021 tarihinde Nakamoto Institute web sitesi: http://web.archive.org/web/20201228100453/https://nakamotoinstitute.org/static/docs/cypherpunk-manifesto.txt adresinden alındı.

Hydra Chain. (2018). Hydra Chain. *Whitepaper*. Hydra Chain.

Iansiti, M., & Lakhani, K. R. (2017, Ocak-Şubat). The truth about Blockchain. *Harvard Business Review*, s. 2701-2709.

ICT Moscow. (2020, 9 16). *Masterchain on ICT Moscow*. 1 15, 2021 tarihinde ICT Moscow web sitesi: http://web.archive.org/save/https://ict.moscow/en/card/masterchain/ adresinden alındı.

IEEE. (2022, 10). *Standards: IEEE Blockchain Initiative*. 10 28, 2022 tarihinde IEEE Blockchain Initiative web sitesi: https://blockchain.ieee.org/standards adresinden alındı.

INFRACHAIN. (2020). *Hakkımızda: Infrachain*. 1 15, 2021 tarihinde Infrachain web sitesi: http://web.archive.org/web/20210115131802/https://infrachain.com/ adresinden alındı.

International Telecommunication Union. (2019). *Focus Group on Application of Distributed Ledger Technology*. 11 29, 2020 tarihinde ITU Web sitesi: http://web.archive.org/web/20201129145602/https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx adresinden alındı.

International Telecommunications Union Telecommunication Standardization Sector (ITU-T). (2019). *Technical Report FG DLT D1.3 Distributed ledger technology standardization.* International Telecommunication Union.

International Telecommunications Union Telecommunication Standardization Sector (ITU-T). (2019). *Technical Report FG DLT D2.1: Distributed ledger technology use cases.* International Telecommunication Union.

International Telecommunications Union Telecommunication Standardization Sector (ITU-T). (2019). *Technical Report FG DLT D5.1 Outlook on distributed ledger technologies.* International Telecommunication Union.

ISO. (2022). *ISO/TC 307 Blockchain and distributed ledger technologies*. 10 28, 2022 tarihinde ISO/TC 307 web sayfası: https://www.iso.org/committee/6266604.html adresinden alındı.

İstanbul Aydın Üniversitesi Blokzincir Uygulama ve Araştırma Merkezi. (2021, 2 26). *Hakkımızda: İstanbul Aydın Üniversitesi Blokzincir Uygulama ve Araştırma Merkezi*. 2 26, 2021 tarihinde İstanbul Aydın Üniversitesi Blokzincir Uygulama ve Araştırma Merkezi web sitesi: https://www.aydin.edu.tr/tr-tr/arastirma/arastirmamerkezleri/blokzincir-uygulama-arastirma-merkezi/Pages/default.aspx adresinden alındı.

Jakobsson, M., & Juels, A. (1999). Proofs of Work and Bread Pudding Protocols (Extended Abstract). B. Preneel içinde, *Secure Information Networks* (s. 258-272). Boston: Springer. doi:https://doi.org/10.1007/978-0-387-35568-9_18..

Kairos Future. (2017). *The Land Registry in the blockchain - testbed.* Stockholm: Kairos Future.

Kakushadze, Z., & Liew, J.-S. (2018, 1). CryptoRuble: From Russia with Love. *SSRN Electronic Journal*, 55-56. doi:10.2139/ssrn.3059330

Kamu İhale Kurumu (KİK). (2022). *Kamu Alımları İzleme Raporu - 2021.* Ankara: KİK Kurumsal Gelişim ve Araştırma Dairesi Başkanlığı.

Karahan, Ç., & Tüfekci, A. (2019). , Blokzincir Teknolojisi ve Kamu Kurumlarınca Verilen Hizmetlerde Blokzincirin Kullanım Durumu. *Verimlilik*, 157-193.

Kelly, M. (2019, 2). Boards Look to Harness Blockchain Disruption. *Tone at the Top*. The Institute of Internal Auditors.

KİK. (2018). *Kamu Alımları İzleme Raporu - 2017.* Ankara: KİK Kurumsal Gelişim ve Araştırma Dairesi Başkanlığı.

KİK. (2019). *Kamu Alımları İzleme Raporu - 2018.* Ankara: KİK Kurumsal Gelişim ve Araştırma Dairesi Başkanlığı.

KİK. (2020). *Kamu Alımları İzleme Raporu - 2019.* Ankara: KİK Kurumsal Gelişim ve Araştırma Dairesi Başkanlığı.

KİK. (2021). *Kamu Alımları İzleme Raporu - 2020.* Ankara: KİK Kurumsal Gelişim ve Araştırma Dairesi Başkanlığı.

Killmeyer, J., White, M., & Chew, B. (2017). *Will blockchain transform the public sector?* Deloitte University Press.

Killmeyer, J., White, M., & Chew, B. (2017). *Will blockchain transform the public sector?* Deloitte University Press.

Kirshbaum, J. (2016, 5 27). *IFTF: Blockchain in High Delta Markets: Manufacturing Trust in Unstable Environments*. 11 17, 2020 tarihinde Institute for the Future (IFTF) Web sitesi: http://web.archive.org/web/20201117131020/https://www.iftf.org/future-now/article-detail/blockchain-in-high-delta-markets-manufacturing-trust-in-unstable-areas/ adresinden alındı.

Koens, T., & Poll, E. (2018). What Blockchain Alternative Do You Need? *International Workshop on Data Privacy Management, Cryptocurrencies and Blockchain Technology* (s. 113–129). Springer.

Kunschke, D., & Henkelmann, S. (2019). Germany. J. Dewey içinde, *Blockchain & Cryptocurrency Regulation* (s. 292). London: Global Legal Group Ltd.

Lamport, L. (1981, 11). Password Authentication with Insecure Communication. *Communications of the ACM, 24*(11), 770-772.

Lamport, L. (2001). Paxos Made Simple. *Computer Science*.

Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems, 4*(3), 382-401.

Lätt, P. (2020). Estonia. J. N. Dewey içinde, *Blockchain & Cryptocurrency Regulation* (s. 332). London: Global Legal Group Ltd.

Ledger Insights. (2020, 7 16). *Beijing uses blockchain for 140 government services*. 11 16, 2020 tarihinde Ledger Insights Web sitesi: http://web.archive.org/web/20201116210315if_/https://www.ledgerinsights.com/beijing-blockchain-140-government-services-publishes-book/ adresinden alındı

Lee, J. M., Yim, S., & Kim, J. Y. (2019). Korea. J. Dewey içinde, *Blockchain & Cryptocurrency Regulation* (s. 367). London: Global Legal Group Ltd.

Leesa-Nguansuk, S. (2017, 8 16). *Rail and Post to use IoT, blockchain*. 1 16, 2021 tarihinde Bangkok Post web sitesi: https://www.bangkokpost.com/business/1307071/rail-and-post-to-use-iot-blockchain adresinden alındı

LeMahieu, C. (2018). Nano: A Feeless Distributed Cryptocurrency Network. *Whitepaper*.

Lerner, B. (2018). *Regulation of Cryptocurrency in Selected Jurisdictions, Iran.* Washington: The Law Library of Congress USA.

Levush, R. (2018). *Regulation of Cryptocurrency in Selected Jurisdictions, Israel.* Washington: The Law Library of Congress USA.

Lin, Y. P., Petway, J. R., Anthony, J., Mukhtar, H., Liao, S. W., Chou, C. F., & Ho, Y. F. (2017). Blockchain: The Evolutionary Next Step for ICT E-Agriculture. *Environments, 4*(3).

Litecoin. (2019, 5 8). *Litecoin Wiki*. 2 28, 2021 tarihinde Litecoin web sitesi: http://web.archive.org/web/20210210221341/https://litecoin.info/index.php/Main_Page adresinden alındı

Liu, Z., Luong, N. C., Wang, W., Niyato, D., Wang, P., Liang, Y.-C., & Kim, D. I. (2019, 3 15). A Survey on Applications of Game Theory in Blockchain. *arXiv.org*, 1-26.

Logith, S., Nitish, P., Raghul, S., & Tamilarasan, T. (2022). Secure Framework for Government Tender Allocation Using Blockchain. *International Research Journal of Modernization in Engineering, Technology and Science*, 884-889.

López-Ibor, A., Stöger, P., & Jin, Z. (2019). Spain. J. Dewey içinde, *Blockchain & Cryptocurrency Regulation* (s. 438). London: Global Legal Group Ltd.

Lubin, J., Anderson, M., & Thomason, B. (2018). Blockchain for Global Development. *Innovations: Technology, Governance, Globalization, 12(1-2)*, 10-17.

Lux, T. (2019, 9 11). FINMA publishes 'stable coin'. *Press Release*. Zürih: FINMA.

Lux, T., & Mathys, V. (2018, 2 16). FINMA publishes ICO guidelines. *Press Release*. Zürih.

LuxTag. (2019, 2 19). *LuxTag's New Solution e-Scroll to Revolutionize Educational Certificates*. 1 16, 2021 tarihinde LuxTag web sitesi: http://web.archive.org/web/20200805133403/https://www.luxtag.io/blog/luxtags-new-solution-e-scroll-to-revolutionize-the-educational-certificates/ adresinden alındı

Lüksemburg Standardizasyon, Akreditasyon ve Ürün ve Hizmet Kalitesi Enstitüsü (ILNAS) ve Standardizasyon ve Bilgi Ekonomisi Ajansı (ANEC). (2018). *Blockchain and Distributed Ledgers.* Lüksemburg: Lüksemburg Ekonomi Bakanlığı.

Lüksemburg Standardizasyon, Akreditasyon ve Ürün ve Hizmet Kalitesi Enstitüsü (ILNAS); Standardizasyon ve Bilgi Ekonomisi Ajansı (ANEC). (2018). *Blockchain and Distributed Ledgers.* Lüksemburg: Lüksemburg Ekonomi Bakanlığı.

Ma, J. (2019). *Draft Project Brief - Settlement Token for Interbank Payments.* Payments Policy Department.

Machado, M., & Abramof, J. F. (2020). Brazil. J. N. Dewey içinde, *Blockchain & Cryptocurrency Regulation* (s. 282). London: Global Legal Group Ltd.

Mali Suçları Araştırma Kurulu (MASAK) Başkanlığı. (2019, 4 12). Şüpheli İşlem Bildirim Rehberi (Bankalar). *MASAK Rehberi*. Ankara: T. C. Hazine ve Maliye Bakanlığı.

Marques, F. L., & Albuquerque, M. (2020). Portugal. J. N. Dewey içinde, *Blockchain & Cryptocurrency Regulation* (s. 476). London: Global Legal Group Ltd.

Martino , W. (2016, 8). Kadena: The first scalable, high performance private blockchain. *Whitepaper*. Kadena LLC.

Martino, W., & Popejoy, S. (2019, 2). The Kadena Public Blockchain. *Project Summary Whitepaper*. Kadena LLC.

Martino, W., Quaintance, M., & Popejoy, S. (2018). Chainweb: A Proof-of-Work Parallel-Chain Architecture for Massive Throughput. *Manuscript*. Kadena LLC.

Maupin, J. (2018). *The G20 Countries Should Engage with Blockchain Technologies to Build an Inclusive, Transparent, and Accountable Digital Economy for All.* Max Planck Institute.

May, T. C. (1994, 12). *Crypto Anarchy and Virtual Communities*. 2 14, 2021 tarihinde Nakamoto Institute web sitesi: http://web.archive.org/web/20201118023716/https://nakamotoinstitute.org/virtual-communities/ adresinden alındı

McLaughlin, M., Ryan, P., & Devlin, C. (2020). Ireland. J. N. Dewey içinde, *Blockchain & Cryptocurrency Regulation* (s. 407). London: Global Legal Group Ltd.

Medipol Üniversitesi. (2018, 2 9). *Medipol Üniversitesi - Haberler - Medipol'de kripto para dersi verilecek*. 5 22, 2018 tarihinde Medipol Üniversitesi - Ana Sayfa: http://www.medipol.edu.tr/Haber/1407/Medipol-de-dijital-para-dersi-verilecek.aspx adresinden alındı

Medipol Üniversitesi. (2022, 8 6). *MEBİS*. 10 29, 2022 tarihinde Medipol Üniversitesi: http://web.archive.org/web/20221029133803/https://mebis.medipol.edu.tr/programbilgi/program/10122 adresinden alındı

Merkle, R. C. (1982). *ABD Patent No. US4309569A.*

Merz, M. (2018). *Enerchain Project Overview and Key Insights.* Hamburg: PONTON GmbH.

Mete, S., Koy, A., & Ersoy, H. (2019). Kriptoparalarda Fiyat Balonu İncelemesi. *BDDK Bankacılık ve Finansal Piyasalar, 13*(1), 105-120.

Miller, D., & Mockel, P. (2019). Using Blockchain to Enable Cleaner, Modern Energy Systems in Emerging Markets. W. B. Corporation içinde, *Blockchain Opportunities for Private Enterprises in Emerging Markets* (s. 59-65). Washington: International Finance Corporation.

Min, C. W., & Yang, C. Z. (2018). *Project Castor: Capital Market Architecture Blueprint in a Decentralised World.* Kuala Lumpur: Securities Commission Malaysia.

Ministry for European Affairs and Equality. (2018, 3 12). *Consultation Paper in relation to the establishment of Malta Digital Innovation Authority (MDIA) and the framework for the cert*. 1 15, 2021 tarihinde Ministry for European Affairs and Equality web sitesi: http://web.archive.org/web/20210115093342/https://meae.gov.mt/en/Public_Consultations/OPM/Pages/Consultations/ConsultationPaperinrelationtotheestablishmentofMaltaDigitalInnovationAuthorityMDIA.aspx adresinden alındı.

Mohite, A., & Acharya, A. (2018). Blockchain for government fund tracking using. *International Conference on Computational Techniques, Electronics and Mechanical Systems (CTEMS)*, (s. 231-234).

Moore, L., & Sawhney, N. (2019). *The West Virginia Mobile Voting Pilot.* Boston: Voatz Inc.

Moore, W., & Stephen, J. (2015, 11 13). *News: Central Bank of Barbados*. 1 16, 2021 tarihinde Central Bank of Barbados web sitesi: http://web.archive.org/web/20210116140856/http://www.centralbank.org.bb/news/article/8827/should-cryptocurrencies-be-included-in-the-portfolio-of-international-reserves adresinden alındı

Moreno, J. D., & Lomaquiz, S. E. (2020). Argentina. J. N. Dewey içinde, *Blockchain & Cryptocurrency Regulation* (s. 245). London: Global Legal Group Ltd.

Moreno, J. D., & Lomaquiz, S. E. (2020). Argentina. J. N. Dewey içinde, *Blockchain & Cryptocurrency Regulation* (s. 245). London: Global Legal Group Ltd.

Mulligan, C. (2018, 4 23). *These 11 questions will help you decide if blockchain is right for your business*. 11 14, 2020 tarihinde World Economic Forum Web sitesi: http://web.archive.org/web/20201114193014/https://www.weforum.org/agenda/2018/04/questions-blockchain-toolkit-right-for-business adresinden alındı

Nakamoto, S. (2008, 10 31). *Bitcoin P2P e-cash paper*. 2 20, 2021 tarihinde metzdowd.com kriptografi e-posta listesi sayfası: http://web.archive.org/web/20210218084142/https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html adresinden alındı

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Bitcoin.org web sitesi: https://bitcoin.org/bitcoin.pdf. adresinden alındı

Nanayakkara, S., Rodrigo, M. N., Perera, S., & Weerasuriya, T. (2021). A Methodology for Selection of a Blockchain Platform to Develop an Enterprise System. *Journal of Industrial Information Integration, 23*(04), 100215.

Niforos, M. (2017). *Blockchain, Opportunities for Private Enterprises in Emerging Markets.* 4. Washington: International Finance Corporation (IFC).

Niforos, M. (2019). Blockchain in Development - How It Can Impact Emerging Markets. W. B. Corporation içinde, *Blockchain Opportunities for Private Enterprises in Emerging Markets* (s. 16-22). Washington: International Finance Corporation.

Nomura Research Institute. (2016). *Survey on Blockchain Technologies and Related Services FY2015 Report.* Tokyo: Japan's Ministry of Economy, Trade and Industry (METI).

Office of the Prime Minister Malta. (2017, 9 28). *Press Releases: Office of the Prime Minister*. 1 15, 2021 tarihinde Malta Başbakanlık Ofisi web sitesi: http://web.archive.org/web/20210115100521/https://www.gov.mt/en/Government/DOI/Press%20Releases/Pages/2017/September/28/pr172207en.aspx adresinden alındı

Office of the Prime Minister Malta. (2018, 5 17). *Press Releases: Office of the Prime Minister*. 1 15, 2021 tarihinde Malta Başbakanlık Ofisi web sitesi: http://web.archive.org/web/20210115095305/https://www.gov.mt/en/Government/DOI/Press%20Releases/Pages/2018/May/17/pr181089.aspx adresinden alındı

Office of the Prime Minister Malta. (2018, 7 12). *Press Releases: Office of the Prime Minister*. 1 15, 2021 tarihinde Malta Başbakanlık Ofisi web sitesi: http://web.archive.org/web/20210115095803/https://www.gov.mt/en/Government/DOI/Press%20Releases/Pages/2018/July/12/pr181566en.aspx adresinden alındı

Office of the Prime Minister Malta. (2019, 2 21). *Press Releases: Office of the Prime Minister*. 1 15, 2021 tarihinde Malta Başbakanlık Ofisi web sitesi: http://web.archive.org/web/20210115094622/https://www.gov.mt/en/Government/DOI/Press%20Releases/Pages/2019/February/21/pr190340.aspx adresinden alındı

Ojo, A., & Adebayo, S. (2017). Blockchain as a Next Generation Government Information Infrastructure: A Review of Initiatives in D5 Countries. A. Ojo, & J. Millard içinde, *Government 3.0 – Next Generation Government Technology Infrastructure and Services* (s. 283-298). Cham: Springer.

Oki, B. M., & Liskov, B. H. (1988). Viewstamped Replication: A New Primary Copy Method to Support Highly-Available Distributed Systems. *PODC '88: Proceedings of the seventh annual ACM Symposium on Principles of distributed computing* (s. 8-17). New York: Association for Computing Machinery.

Ølnes, S., & Jansen, A. (2018). Blockchain Technology as Infrastructure in Public Sector – an Analytical Framework. *19th Annual International Conference on Digital Government Research Governance in the Data Age - Dgo*, (s. Article No.: 77, pp 1-10). Delft.

Ongaro, D., & Ousterhout, J. (2014). *In Search of an Understandable Consensus Algorithm.* Stanford : Stanford University.

OpenChain Project. (2016). Open Chain. *Yellow Paper*. The Linux Foundation.

Panpatte, S., & Takale, V. D. (2019, Şubat). To Study the Decision Making Process in an Organization for its Effectiveness. *The International Journal of Business Management and Technology, 3*(1), 73-78.

Parliamentary Secretariat for Financial Services, Digital Economy and Innovation Office of the Prime Minister. (2018, 2 16). Consultation Document. *The establishment of the Malta Digital Innovation Authority; the Framework for the Certification of Distributed Ledger Technology Platforms and Related Service Providers; and a Virtual Currency Act* . Malta: Office of the Prime Minister (Malta).

Pascual, J., Holle, H., & Petit, C. (2020, 10 23). *Blockchain Laws and Regulations, Luxembourg*. 10 26, 2020 tarihinde Global Legal Insights web sitesi: https://web.archive.org/web/20201026125919/https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/luxembourg adresinden alındı

Peck, M. E. (2012, 5 30). *Bitcoin: The Cryptoanarchists' Answer to Cash*. 2 15, 2021 tarihinde Spectrum IEEE web sitesi: http://web.archive.org/web/20201219184314if_/https://spectrum.ieee.org/computing/software/bitcoin-the-cryptoanarchists-answer-to-cash adresinden alındı

Perchet, C., Loget, J., & Daniel, S. (2020). France. J. N. Dewey içinde, *Blockchain & Cryptocurrency Regulation* (s. 344). London: Global Legal Group Ltd.

Perley, B. (2017, 10 27). *Crypto-Governance and the Dangers of Faction*. 2 24, 2021 tarihinde Medium.com web sitesi: http://web.archive.org/web/20210224205512/https://medium.com/@BuckPerley/crypto-governance-f1318affbbe0 adresinden alındı

Pipan, R. (2017, 2 7). *The Bitfury Group and Government of Republic of Georgia Expand Historic Blockchain Land-Titling Project*. Tbilisi, Georgia: Bitfury.

Popejoy, S. (2016, 8). Confidentiality in Private Blockchain. *Whitepaper*. Kadena LLC.

Port of Antwerp. (2017, 6 28). *Antwerp start-up T-Mining develops Blockchain solution for safe, efficient container release*. 1 16, 2021 tarihinde Port of Antwerp web sitesi: http://web.archive.org/web/20210116111942/https://www.portofantwerp.com/en/news/antwerp-start-t-mining-develops-blockchain-solution-safe-efficient-container-release adresinden alındı

Power Ledger. (2019). Power Ledger White Paper. *White Paper*. Australia: Power Ledger.

Power Ledger. (2019, 12 18). *Virtual Power Plant project*. 10 12, 2020 tarihinde Power Ledger Web sitesi: https://www.powerledger.io/announcement/power-ledger-powerclub-sonnen-and-natural-solar-team-up-to-save-australians-thousands-through-virtual-power-plant-project/ adresinden alındı

Probst, L., Frideres, L., Cambier, B., & Martinez-Diaz, C. (2016). *Blockchain applications & services.* Business Innovation Observatory. Brussels: European Commission.

Procivis AG. (2019, 2 6). *What is eID+?* 1 14, 2021 tarihinde Procivis - E-government as a Service: https://web.archive.org/web/20210114200948/https://procivis.ch/eid/ adresinden alındı

Psaila, S. (2017). *Blockchain: A game changer for audit.* Malta: Deloitte.

Quaintance, M., & Martino, W. (2018). Chainweb Protocol Security Calculations. *Whitepaper Draft v7*. Kadena LLC.

Raikwar, M., Gligoroski, D., & Kralevska, K. (2019). SoK of Used Cryptography in Blockchain. *https://eprint.iacr.org/*. International Association for Cryptologic Research (IACR).

Ramachandran, V., & Rehermann, T. (2019). Can Blockchain Technology Address De-Risking in Emerging Markets? W. B. Corporation içinde, *Blockchain Opportunities for Private Enterprises in Emerging Markets* (s. 23-28). Washington: International Finance Corporation.

Ramanathan, A., Tiwari, A., & Rautray, R. (2019). India. J. Dewey içinde, *Blockchain & Cryptocurrency Regulation* (s. 335). London: Global Legal Group Ltd.

Rao , R. V. (2008). Evaluating flexible manufacturing systems using a combined multiple attribute decision making method . *International Journal of Production Research*(46(7)), 1975–1989.

Rath, U., & Kulnigg, T. (2020). Austria. J. N. Dewey içinde, *Blockchain & Cryptocurrency Regulation* (s. 263). London: Global Legal Group Ltd.

Reeves, P. (2020). Australia. J. N. Dewey içinde, *Blockchain & Cryptocurrency Regulation* (s. 251). London: Global Legal Group Ltd.

Ribeiro, S. L., & Nakamura, E. T. (2019). Context-Based Blockchain Platform Definition and Analysis Methodology. *Advances in Cyber Security, First International Conference, ACeS 2019* (s. 74-89). Penang, Malaysia: Springer.

Richards, T. (2018, 6 26). Cryptocurrencies and Distributed Ledger Technology. *Australian Business Economists Briefing*. Sydney, Australia: Reserve Bank of Australia.

Rodriguez-Ferrand, G. (2018). *Regulation of Cryptocurrency in Selected Jurisdictions, Argentina.* Washington: The Law Library of Congress USA.

Rogers, E. M. (1983). *Diffusion of Innovations* (3. b.). New York: A Division of Macmillan Publishing Co., Inc.

Rooney, H., Aiken, B., & Rooney, M. (2017). Q&A. Is Internal Audit Ready for Blockchain? *Technology Innovation Management Review*, 7(10): 41-44.

Russian National Settlement Depository (NSD). (2016, 11 10). *NSD and iCoinSoft Develop Solutions for Blockchain Assets Circulation*. 1 15, 2021 tarihinde National Settlement Depository web sitesi: http://web.archive.org/web/20200926111240/https://www.nsd.ru/en/publications/news/press-releases/nsd-and-icoinsoft-develop-solutions-for-blockchain-assets-circulation-2016-11-10_115100/ adresinden alındı

Russian National Settlement Depository (NSD). (2018, 5 15). *Altoros NSC Commercial Paper About Decentralized Depository Instruction Management on Blockchain*. 1 15, 2021 tarihinde Github web sitesi: http://web.archive.org/web/20210115201948/https://github.com/Altoros/nsd-commercial-paper adresinden alındı

Russian National Settlement Depository (NSD). (2018, 10 1). *Media about us: NSD*. 1 15, 2021 tarihinde National Settlement Depository (NSD) web sitesi: http://web.archive.org/web/20200925194116/https://www.nsd.ru/en/publications/news/media-about-us/nsd-leads-blockchain-implementation-in-russia-2018-10-01_103600/ adresinden alındı

Saaty, R. W. (1987). The analytic hierarchy process—what it is and how it is used. *Mathematical Modelling, 9*(3-5), 161-176. doi:10.1016/0270-0255(87)90473-8

Saaty, T. L. (1980). *The Analytic Hierarchy Process.* New York: NY: McGraw-Hill.

Salmon, J., & Myers, G. (2019). Blockchain and Associated Legal Issues for Emerging Markets. W. B. Corporation içinde, *Blockchain Opportunities for Private Enterprises in Emerging Markets* (s. 66-75). Washington: International Finance Corporation.

Schep, B., Godlieb, C., & Röell, W. (2019). Netherlands. J. Dewey içinde, *Blockchain & Cryptocurrency Regulation* (s. 395). London: Global Legal Group Ltd.

Sekniqi, K., Laine, D., Buttolph, S., & Sirer, E. G. (2020, 6 30). Avalanche Platform. *Ava Labs Whitepapers*. ABD: Ava Labs.

Sheldon, M. D. (2018, 12 5). A Primer for Information Technology General Control Considerations on a Private and Permissioned Blockchain Audit. *American Accounting Association Journal*.

Shin, L. (2017, 2 7). *The First Government To Secure Land Titles On The Bitcoin Blockchain Expands Project*. 1 16, 2021 tarihinde Forbes web sitesi: http://web.archive.org/web/20210116132709/https://www.forbes.com/sites/laurashin/2017/02/07/the-first-government-to-secure-land-titles-on-the-bitcoin-blockchain-expands-project/?sh=60357b3b4dcd adresinden alındı

Shuaib, M., Daud, S. M., Alam, S., & Khan, W. Z. (2020). Blockchain-based framework for secure and reliable land registry system. *TELKOMNIKA Telecommunication, Computing, Electronics and Control, 18*(5), 2560-2571. doi:10.12928/TELKOMNIKA.v18i5.15787

Siassiakos, K., Ilioudi, S., Effrosyni, T., Mitsiou, V., & Nanouris, D. (2020). Utilization of Blockchain Technology in Greek Public Administration. *Advances in Management & Applied Economics, 10*(4), 223-237.

Six, N., Herbaut, N., & Salinesi, C. (2020, 4 9). Quelle Blockchain choisir ? Un outil d'aide à la décision pour guider le choix de technologie Blockchain. *arXiv:2004.06080*, 1-16.

Smartmatic. (2015, 12). *Chile at the forefront of online voting optimizing citizen participation*. 1 15, 2021 tarihinde TIVI web sitesi: http://web.archive.org/web/20210115133035/https://tivi.io/case/chile-2015/ adresinden alındı

Smith, A. M. (2018, 3 15). *The blockchain challenge nobody is talking about*. 3 26, 2019 tarihinde PwC Next in Tech: https://usblogs.pwc.com/emerging-technology/the-blockchain-challenge/ adresinden alındı

Smolenski, N. (2017). *Blockchain in Government Briefing: Q3 2017.* Dallas, Texas: Learning Machine.

Soares, E. (2018). *Regulation of Cryptocurrency in Selected Jurisdictions, Brazil.* Washington: The Law Library of Congress USA.

Standards Australia. (2017). *Roadmap for Blockchain Standards.* Sydney: Standards Australia.

(2017). *Stellar Development Foundation; The Luxembourg House of Financial Technology.* San Francisco: Stellar Development Foundation.

Strizh, V., Dmitriev, D., & Kiseleva, A. (2020). Russia. J. N. Dewey içinde, *Blockchain & Cryptocurrency Regulation* (s. 486). London: Global Legal Group Ltd.

Suichies, B. (2015, 12 21). *Why Blockchain must die in 2016?* 11 10, 2020 tarihinde Medium Web sitesi: http://web.archive.org/web/20201110194627/https://medium.com/block-chain/why-blockchain-must-die-in-2016-e992774c03b4 adresinden alındı

Szabo, N. (1996). *Smart Contracts: Building Blocks for Digital Markets*. 11 9, 2020 tarihinde Phonetic Sciences Web sitesi: http://web.archive.org/web/20201109130159/https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html adresinden alındı

Szabo, N. (2005, 12 29). *Bit Gold*. 2 15, 2021 tarihinde Nakamoto Institute web sitesi: http://web.archive.org/web/20210128070221/https://nakamotoinstitute.org/bit-gold/ adresinden alındı

T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı. (2019, 11 3). 2020 Yılı Cumhurbaşkanlığı Yıllık Programı. *Cumhurbaşkanlığı Yıllık Programları*. Ankara: T. C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı.

T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı. (2019, 7). On Birinci Kalkınma Planı (2019-2023). *Kalkınma Planı*. Ankara: T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı.

T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı. (2020, 10 26). 2021 Yılı Cumhurbaşkanlığı Yıllık Programı. *Cumhurbaşkanlığı Yıllık Programları*. Ankara: T. C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı.

T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı. (2021, 10 25). 2022 Yılı Cumhurbaşkanlığı Yıllık Programı. *Cumhurbaşkanlığı Yıllık Programları*. Ankara: T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı.

T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı. (2022, 10 25). 2023 Yılı Cumhurbaşkanlığı Yıllık Programı. *Cumhurbaşkanlığı Yıllık Programları*. Ankara: T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı.

T.C. Sanayi ve Teknoloji Bakanlığı. (2019, 9 18). 2023 Sanayi ve Teknoloji Stratejisi. *Strateji Belgesi* . Ankara: T.C. Sanayi ve Teknoloji Bakanlığı.

T.C. Ticaret Bakanlığı. (2019, 1 10). *Haberler: Ticaret Bakanlığı*. Ticaret Bakanlığı web sitesi: http://web.archive.org/web/20210126210841/https://www.ticaret.gov.tr/haberler/ihracat-blokzincir-teknolojisiyle-hizlanacak adresinden alındı

T.C. Ticaret Bakanlığı. (2020, 12 30). *DigiKamp Dijital Dönüşüm Yarışması Şartnamesi*. DigiKamp web sitesi: http://web.archive.org/web/20210126211437/https://www.digikamp.gov.tr/Content/files/Digikamp-Teknik-Sartnamesi.pdf adresinden alındı

Tasmu Digital Valley. (2019). *What is TASMU Digital Valley?* 1 16, 2021 tarihinde Tasmu Digital Valley web sitesi: http://web.archive.org/web/20210116133129/https://tdv.motc.gov.qa/tasmu-digital-valley-services adresinden alındı

Tendermint Inc. (tarih yok). *What is Tendermint*. 4 14, 2021 tarihinde Tendermint Core web sitesi: http://web.archive.org/web/20210127071755/https://docs.tendermint.com/master/introduction/what-is-tendermint.html adresinden alındı

The Law Library of Congress, Global Legal Research Center. (2018). *Regulation of Cryptocurrency Around the World.* Washington: The Law Library of Congress.

The University of British Columbia. (2017). *The BC Land Titles and Survey Authority (LTSA) Digital ID Design Challenge*. 1 15, 2021 tarihinde The University of British Columbia web sitesi: http://web.archive.org/web/20210115121349/https://blockchain.ubc.ca/research/bc-land-title-survey-authority-ltsa-digital-id-design-challenge-diac adresinden alındı

The World Bank. (2017). *Financial Sector Support Project (P151816) Implementation Status & Results Report.* Kenya: The World Bank.

Tobor, N. (2016, 11 24). *Senegal To Introduce A New Blockchain-Based National Digital Currency, The Second Such Currency In The World*. 1 16, 2021 tarihinde iAfrikan web sitesi: http://web.archive.org/web/20201214021502/https://www.iafrikan.com/2016/11/24/s

enegal-to-introduce-a-new-blockchain-based-national-digital-currency-making-it-only-the-second-country-to-have-a-national-digital-currency/ adresinden alındı

Triantaphyllou, E., & Mann, S. H. (1994). A Computational Evaluation of the Original and Revised Analytic Hierarchy Process. *Computers and Industrial Engineering, 26*(3), 609-618.

Uludağ, A. S., & Doğan, H. (2016). Çok Kriterli Karar Verme Yöntemlerinin Karşılaştırılmasına Odaklı Bir Hizmet Kalitesi Uygulaması. *Çankırı Karatekin Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 6*(2), 17-47.

Umeda, S. (2018). *Regulation of Cryptocurrency in Selected Jurisdictions, Japan.* Washington: The Law Library of Congress USA.

UN Economic Commission for Latin America and the Caribbean. (2019). *Submissions from entities in the United Nations system and elsewhere on their efforts in 2018 to implement the outcome of the WSIS.* Geneva: UN Commission on Science and Technology for Development (CSTD).

United Nations Innovation Network. (2020). *A Practical Guide to Using Blockchain within the United Nations.* United Nations.

USA Homeland Security Department. (2016, 6 17). *S&T Awards $199K to Austin Based Factom Inc. for IoT Systems Security*. 1 14, 2021 tarihinde Homeland Security: http://web.archive.org/web/20210114164442/https://www.dhs.gov/science-and-technology/news/2016/06/17/st-awards-199k-austin-based-factom-inc-iot-systems-security adresinden alındı

Usta, A., & Doğantekin, S. (2017). *Blockchain 101.* İstanbul: Kapital Medya Hizmetleri A.Ş.

Valkenburgh, P. V. (2017, 10 17). *What is "open source" and why is it important?* 2 27, 2021 tarihinde Coincenter.org web sayfası: http://web.archive.org/web/20210227205747/https://www.coincenter.org/education/advanced-topics/open-source/ adresinden alındı

Wall, E., & Malm, G. (2016, 6 29). Lisans Tezi. *Using Blockchain Technology and Smart Contracts to Create a Distributed Securities Depository*. Lund, İsveç: Lund University.

Walport, M. (2016). *Distributed Ledger Technology: beyond block chain.* Londra: UK Government Office for Science.

Walport, M. (2016). *Distributed Ledger Technology: beyond block chain.* Londra: UK Government Office for Science.

White, L. H. (2014, 3 10). The Troubling Suppression of Competition from Alternative Monies: The Cases of the Liberty Dollar and E-gold. *GMU Working Paper in Economics No. 14-06*. USA: George Mason University Department of Economics. SSRN: https://ssrn.com/abstract=2406983 adresinden alındı

Windarto, A. P., & Muhammad, A. (2017). Comparison of Weighted Sum Model and Multi Attribute Decision Making Weighted Product Methods in Selecting the Best

Elementary School in Indonesia. *International Journal of Software Engineering and Its Applications, 11*(4), 69-90.

Wood, G. (2016). Polkadot: Vision for a Heterogeneous Multi-Chain Framework. *Whitepaper Darft-1*. Parity.

World Bank. (2019). *ID4D Practitioner's Guide: Version 1.0.* Washington, D.C.: World Bank.

World Economic Forum. (2018). *Building Block(chain)s for a Better Planet.* San Francisco: World Economic Forum.

World Food Programme. (2020, 11 8). *Building Blocks | WFP Innovation*. 10 11, 2020 tarihinde World Food Programme Innovation Web sitesi: http://web.archive.org/web/20201102143609/https://innovation.wfp.org/project/building-blocks adresinden alındı

Wüst, K., & Gervais, A. (2018). Do you need a Blockchain? *Crypto Valley Conference on Blockchain Technology (CVCBT)* (s. 45-54). Zug: IEEE. doi:10.1109/CVCBT.2018.00011

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). *Blockchain Technology Overview.* United States National Institute of Standards and Technology.

Yang, D., Gavigan, J., & Wilcox-O'Hearn, Z. (2016). *Survey of Confidentiality and Privacy Preserving Technologies for Blockchains.* R3.

Yin, M., Sekniqi, K., van Renesse, R., & Sirer, E. G. (2020, 8 24). Scalable and Probabilistic Leaderless BFT Consensus through Metastability. *arXiv*(arXiv:1906.08936v2), 1-21.

Žarkovič, V. (2019, 12 16). *Slovenia Launched national test blockchain infrastructure and Slovenian Blockchain partnership*. 1 15, 2021 tarihinde Slovenya Devlet İletişim Ofisi web sitesi: http://web.archive.org/web/20201020010225/https://slovenia.si/business-and-innovation/slovenia-launched-national-test-blockchain-infrastructure-and-slovenian-blockchain-partnership/ adresinden alındı

Zhang, L. (2018). *Regulation of Cryptocurrency in Selected Jurisdictions, China.* Washington: The Law Library of Congress USA.

ZIGURAT İnovasyon ve Teknoloji Okulu. (2019). *Governments' Blockchain Initiatives*. 1 15, 2021 tarihinde E-zigurat web sitesi: http://web.archive.org/web/20210115141040/https://www.e-zigurat.com/innovation-school/blog/governments-blockchain-initiatives/ adresinden alındı.

EKLER

EK-1. Süreç Bilgi Formu

Aşağıdaki sorular ilgili sürece göre uygun biçimde doldurulacaktır.

1. Kullanım senaryosu, birden fazla kurumu/birimi içeren bir iş ağını kapsıyor mı?

   ○ Evet
   ○ Hayir

   Eğer yanıt "evet" ise aşağıdaki tabloyu uygun biçimde doldurunuz (*ihtiyaca göre tabloya sütun ve/veya satır ilave edilebilir*). Yanıt "hayır" ise blokzincir kullanımı önerilmemektedir.

Çizelge 1.1. Süreçte rol alan kurum/birimler ve rolleri

Rol / Kurum/birim	Bilgi sağlayan	Bilgi onaylayan/ doğrulayan	Bilgi sorgulayan	Bilgi kullanan	Bilginin sahibi
…					

2. Süreç işlem hacmi, veri temin edilebilmesi halinde önceki yıllara ait değerler ile geleceğe ilişkin tahminler Çizelge 1.2'ye göre doldurulacaktır.

   İşlem hacmi; belirli bir zaman diliminde (saniye, saat, gün vb.) gerçekleştirilebilen işlem miktarını ifade etmektedir.

Çizelge 1.2. Süreç işlem hacmi

İşlem sayısı (adet)	Saatlik	Günlük	Haftalık	Aylık	Yıllık
Min					
Ort					
Max					

3. Süreç tarafından üretilen/depolanan veri miktarı (tahmini ya da ölçüm değeri)

   Biriken verinin hacminin artması ile ilgili olarak belirli bir zaman periyodu sonrasında depolanacak veri hacmi tahmin edilmeli ve alınacak önlemler netleştirilmelidir.

Çizelge 1.3. Süreç tarafından üretilen/depolanan veri miktarı

	A	B	C	D	E	F
	İşlem veri boyutu (byte)	Saatte işlem sayısı (adet)	Günlük işlem veri boyutu (AxBx24)	Günlük (mb) [C/(1024x1024)]	Aylık (mb) (Dx31)	Yıllık (gb) (Dx365/1024)
Min						
Ort						
Max						

EK-1. (devam) Süreç Bilgi Formu

4. Süreç işlem hızı (mevcut/istenen/max/min) veri temin edilebilmesi halinde mevcut değerler ile geleceğe ilişkin tahminler Çizelge 1.4'e göre doldurulacaktır. Burada ayrıca ağ gecikmesi ya da işlem gecikme toleransı ile birlikte anlık işlem doğrulamanın gerekli olup olmadığı da belirtilecektir.

   İşlem hızı; bir işlem için gerçekleşen talep ile o işlemin sonuçlanması arasında geçen süreyi ifade etmektedir. İşlem hızı aynı zamanda blok onaylanma zamanı ile de ilişkilidir. Blok onaylanma zamanı, bir işlemin ağa düşmesi ile bloğun yaratılması arasında geçen süredir.

Çizelge 1.4. Süreç işlem hızı

İşlem hızı	Mevcut durum	Beklenen durum	İşlem gecikme toleransı	Anlık işlem doğrulama gerekli mi?
Min				
Ort				
Max				

5. Sürecin özellikleri dikkate alınarak blokzincir üçlü açmazı olarak da bilinen üç niteliğe ilişkin değerlendirme Çizelge 1.5'e göre yapılacaktır. Bu çizelgede, verilen üç özelliğin önem derecesi en önemli 3, en düşük önemli 1 olmak üzere belirtilecektir.

Çizelge 1.5. Blokzincir üçlü açmazına göre niteliklerin önem dereceleri

Nitelik	Açıklama	Önem derecesi
Ölçeklenebilirlik	Ölçeklenebilirlik, artan ya da genişleyen iş yükü ya da kapsamına karşılık performans ve verimliliğin korunması demektir. Örnek süreç zamana bağlı olarak kullanıcı sayısı artan bir süreçtir ve gelecekte işlem hacminin artması beklenmektedir. Bu nedenle ölçeklenebilirlik özelliği önem taşımaktadır.	
Merkezsizlik	Örnek süreç bir kamu kurumu tarafından sunulan bir hizmet olduğundan merkezsizlik gereksinimi nispeten daha az önem taşımaktadır.	
Güvenlik	İçerdiği veriler ve kullanıcı bilgileri nedeni ile asgari olarak bir veri tabanının sunduğu güvenlik düzeyi beklenmektedir.	

6. Süreç veri içeriği; sistemde saklanacak olan veri ve metaveriyi tanımlamaktadır. Bu bilgi sürece bağlı olarak her türlü bilgi olabilir. Süreç içerisinde blokzincire kaydedilecek olan veriler, Çizelge 1.6'da verilen şablona uygun biçimde listelenecektir.

   Metaveri, blokzincirde tutulan veriyi tanımlayan, bir başka deyişle verinin kaynağı, formatı, kalitesi gibi niteliklerini açıklayan veridir.

EK-1. (devam) Süreç Bilgi Formu

Çizelge 1.6. Süreç veri içeriği

	Veri	Boyut	Açıklama
	Blok #	4 byte	Blok numarası
	Blok Boyutu	4 byte	Bu alanı takip eden bloğun boyutu
	Önceki bloğun hash değeri	32 byte	Zincirdeki önceki bloğun (parent) hash referansı
	Merkle Ağacı	32 byte	Bu bloktaki işlemlerin Merkle ağacının kökünün hash değeri
	Zaman damgası	4 byte	Bloğun yaklaşık yaratılma zamanı (Unix Epoch saniye)
	İşlem sayısı	4 byte	Bloğun içerdiği işlemlerin adedi
Süreç Bilgileri	…		
	…		
	…		

7. Veri sınıflandırma; Süreçte kullanılan, üretilen ve depolanan verilerin sınıflandırılmasına ilişkin bilgileri içermektedir. Buna göre veriler aşağıdaki biçimde sınıflandırılacaktır:
    - Herkese açık veriler: İstisnasız herkesin erişip görüntüleyebileceği özellikteki verileri ifade etmektedir.
    - Özel veriler: Sadece belirli kullanıcıların görüntüleyebileceği özellikteki verileri ifade etmektedir.
    - İzne tabi veriler: Erişimin izne tabi olduğu özellikteki verileri ifade etmektedir.

Çizelge 1.7. Süreç verilerinin sınıflandırılması

	Veri	Veri sınıfı
	Blok #	Herkese açık
	Blok Boyutu	Herkese açık
	Önceki bloğun hash değeri	Herkese açık
	Merkle Ağacı	Herkese açık
	Zaman damgası	Herkese açık
Süreç Bilgileri	…	
	…	
	…	
	…	

8. Sürecin işleyişi: Süreç tüm faaliyet, alt faaliyet ve alt süreçleri ile birlikte detaylı biçimde tanımlanacaktır. Bu tanımlama işlem adımları ve/veya akış şeması biçiminde olacak, her bir adım birinci maddede listelenmiş olan roller ile ilişkilendirilecektir.

EK-1. (devam) Süreç Bilgi Formu

9. Hassas, gizli ya da kritik bilgi ya da veri kullanımı; süreç içerisinde kişisel bilgiler, sağlık verileri, gizlilik dereceli veriler gibi hassas veriler kullanılıyorsa belirtilecektir.

10. Dış bilgi gereksinimi; süreç içerisinde sensör, IoT, elle veri girişi gibi dış veriler kullanılıyorsa bunlar belirtilecektir.

11. Mevcut mevzuat; sürece ilişkin varsa yasal düzenlemeler belirtilecektir. Bu yasal düzenlemeler kanun, yönetmelik, yönerge, talimat, standart olabileceği gibi kurum içi düzenleme de olabilecektir. Eğer sürecin işleyişi bir kalite dokümanına dayanıyorsa bu dokümana referans verilecektir.

12. Fonksiyonel gereksinimler; Bu gereksinimler blokzincire dayalı sistemin gerçekleştirmesi ya da başarması gereken özelliklerdir. Bir başka ifade ile, sistemin vermesi gereken hizmetlerdir ve sistemin ne yapması gerektiğini açıklarlar.

Çizelge 1.8. Fonksiyonel gereksinimler

Gereksinim	**Sürece uygunluk**	**Açıklama**
Ortak ve tutarlı veri saklama	□ Evet □ Hayır	
Birden fazla kullanıcının kayıt yazabilmesi	□ Evet □ Hayır	
Tüm kayıt ekleyebilen aktörler arasında güven ve hiyerarşi eksikliği	□ Evet □ Hayır	
Aracı ya da merkezi otorite bulunmaması	□ Evet □ Hayır	
Kayıtların değiştirilememesi, silinememesi, güncellenememesi	□ Evet □ Hayır	
Katılımcıların belirlenen düzeyde anonimliğe sahip olması	□ Evet □ Hayır	

EK-1. (devam) Süreç Bilgi Formu

13. Fonksiyonel olmayan gereksinimler; Bu gereksinimler sistemin beklenen özelliklerini tanımlamaktadır. Sistemin kalite özelliklerini tanımlar, sistem kısıtlarını ve olması beklenen durumu tarif ederler. Fonksiyonel olmayan gereksinimler karşılanmadığı takdirde sistem kullanışsız hale gelebilir.

Çizelge 1.9. Fonksiyonel olmayan gereksinimler

Gereksinim	Süreç için kritiklik	Açıklama
Ölçeklenebilirlik	□ Düşük □ Orta □Yüksek	
İşlem hızı	□ Düşük □ Orta □Yüksek	
İşlem hacmi	□ Düşük □ Orta □Yüksek	
Sistem güvenliği (çatallanma, mutabakat mekanizması açıkları)	□ Düşük □ Orta □Yüksek	
Diğer sistemlerle entegrasyon	□ Düşük □ Orta □Yüksek	
Verimlilik	□ Düşük □ Orta □Yüksek	
Mevzuat düzenlemelerine uyum	□ Düşük □ Orta □Yüksek	
Teknik ve süreç olgunluk/ standardizasyon düzeyi	□ Düşük □ Orta □Yüksek	
Şeffaflık	□ Düşük □ Orta □Yüksek	

14. Mevcut süreç/faaliyetle ilgili problemler ya da iyileştirilebilir noktalar; blokzincir çözümünün uygulanacağı sürecin mevcut durumundaki problemler, darboğazlar ve iyileştirilebilir alanlar bu kısımda, aşağıdaki tablo kullanılarak listelenecektir. Tabloda örnek olarak bazı durumlar verilmiştir.

Çizelge 1.10. Mevcut süreç/faaliyetle ilgili problemler ya da iyileştirilebilir noktalar

Mevcut problem-darboğaz-iyileştirilebilir alan	Tipi (Problem, iyileştirilebilir alan)	Blokzincirden faydalanılabilir mi?
	□ Problem □ İyileştirilebilir alan	□ Evet □ Hayır
	□ Problem □ İyileştirilebilir alan	□ Evet □ Hayır
	□ Problem □ İyileştirilebilir alan	□ Evet □ Hayır
	□ Problem □ İyileştirilebilir alan	□ Evet □ Hayır
	□ Problem □ İyileştirilebilir alan	□ Evet □ Hayır

EK-2. Süreç Bilgi Formu (Kamu İhale Süreci)

1. Kullanım senaryosu, birden fazla kurumu/birimi içeren bir iş ağını kapsıyor mı?

○ Evet
○ Hayir

Çizelge 2.1. Süreçte rol alan kurum/birimler ve rolleri (Kamu İhale Süreci)

Rol / Kurum/birim	Bilgi sağlayan	Bilgi onaylayan/ doğrulayan	Bilgi sorgulayan	Bilgi kullanan	Bilginin sahibi
İhaleyi gerçekleştiren	✓	✓	✓	✓	✓
İhale dokümanını satın alan(lar)				✓	
Teklif veren(ler) – Yüklenici adayları	✓			✓	✓
Alt Yüklenici adayları	✓			✓	
Teklif değerlendirme heyeti		✓	✓	✓	
Yüklenici	✓			✓	✓
Alt yüklenici(ler)	✓				✓

Kamu ihale sürecinde yer alan taraflar sürecin farklı aşamalarında farklı görevler ve sorumluluklar üstlenmekte, bazı roller ise paylaşılmaktadır.

2. Süreç işlem hacmi, veri temin edilebilmesi halinde önceki yıllara ait değerler ile geleceğe ilişkin tahminler Çizelge 1.2'ye göre doldurulacaktır (işlem adedine göre, saniyede, dakikada ya da saatte işlem sayısı).

Kamu İhale Kurumu'nun 2021 yılı Kamu Alımları İzleme Raporuna göre (Kamu İhale Kurumu (KİK), 2022) 2021 yılı içinde ihale yapan idare sayısı 9 053, ihale sayısı ise 86 711 olarak gerçekleşmiştir. Bu ihalelerden 25 943'ü ihale tarihinden sonra iptal edilmiş olmakla birlikte, süreç başlatılmış ve belirli bir aşamaya getirilmiş olduğundan iptal edilen ihale sayısı dikkate alınmayarak bir kurum için yıllık ihale sayısı toplam ihale sayısının toplam idare sayısına bölünmesi ile yaklaşık olarak 10 (9,58) bulunmuştur.

Kamu İhale Kurumu'nun 2020 yılı Kamu Alımları İzleme Raporuna göre (KİK, 2021) 2020 yılında ihale yapan idare sayısı 8 923, ihale sayısı 100 350 olarak gerçekleşmiştir. Buna göre, idare başına ortalama ihale sayısı 12 (11,25) olarak hesaplanmıştır.

Kamu İhale Kurumu'nun 2019 yılı Kamu Alımları İzleme Raporuna göre (KİK, 2020) 2019 yılı içinde ihale yapan idare sayısı 9 524, ihale sayısı 95 109 olarak gerçekleşmiştir. Buna göre, idare başına ortalama ihale sayısı 10 (9,99) olarak hesaplanmıştır.

EK-2. (devam) Süreç Bilgi Formu (Kamu İhale Süreci)

Kamu İhale Kurumu'nun 2018 yılı Kamu Alımları İzleme Raporuna göre (KİK, 2019) 2018 yılı içinde ihale yapan idare sayısı 10 769, ihale sayısı 112 446'dır. Buna göre, idare başına ortalama ihale sayısı 11 (10,44) olarak hesaplanmıştır.

Kamu İhale Kurumu'nun 2017 yılı Kamu Alımları İzleme Raporuna göre (KİK, 2018) 2017 yılı içinde ihale yapan idare sayısı 12 283, ihale sayısı 135 260'tır. Buna göre, idare başına ortalama ihale sayısı 12 (11,01) olarak hesaplanmıştır.

Benzer biçimde KİK yıllık izleme raporlarından alınan değerlere göre 2011 – 2021 yılları arasındaki ihale sayıları ve idare sayıları (bu sayılara daha sonra iptal edilmiş olan ihaleler de dâhildir) Çizelge 2.2.'de verilmiştir.

Çizelge 2.2. Süreç işlem hacmi (Kamu İhale Süreci)

Yıl	İhale sayısı	İdare sayısı	Ortalama	Yaklaşık	Minimum	Ortalama	Maksimum
2021	86.711	9.053	9,58	10	-	10	-
2020	100.350	8.923	11,25	12	-	12	-
2019	95.109	9.524	9,99	10	-	10	-
2018	112.446	10.769	10,44	11	-	11	-
2017	135.260	12.283	11,01	12	-	12	-
2016	160.437	12.299	13,04	14	-	14	-
2015	164.327	12.211	13,46	14	-	14	-
2014	157.879	12.974	12,17	13	-	13	-
2013	175.724	12.960	13,56	14	-	14	-
2012	141.731	11.944	11,87	12	-	12	-
2011	213.587	15.914	13,42	14	-	14	-

3. Süreç tarafından üretilen/depolanan veri miktarı (tahmini ya da ölçüm değeri)

Kamu ihale süreci için işlem sayısı herhangi bir finansal işlem kadar yoğun olmadığından işlemlerin boyutu önemli bir kısıt oluşturmamaktadır. Süreç içerisinde üretilen ve depolanan veriler ihaleye ilişkin teknik ve idari şartname ya da Teklife Çağrı Dosyasını, ihaleye katılım şartlarını (ihale duyurusunda yer alan koşullar), yüklenici adayları tarafından hazırlanan teklifleri ve banka dekontu gibi eklerini içermektedir. Ancak, işin ve/veya ilgili kurumların özelliğine göre bu verilerin gizlilik-güvenlik gereksinimi nedeni ile blokzincir ağında saklanmasının istenmemesi halinde bu dokümanların zincir dışında (off-chain) tutulup blokzincirde sadece adres ya da özet bilgilerinin paylaşılması da mümkündür.

EK-2. (devam) Süreç Bilgi Formu (Kamu İhale Süreci)

Kamu ihale süreci için, veri miktarı tahmini yapılırken bir kurumun hazırlamış olduğu 41 adet ihale dokümanının boyutlarının ortalaması alınmış, MS Word ve pfd dosya biçiminden oluşan bu dokümanların ortalama 10 mb civarında olduğu tespit edilmiştir.

Veri boyutu hesaplanırken, her bir ihale için 10 mb boyutundaki dosya boyutu yılda gerçekleştirilen ihale sayısı ile çarpılmakta, daha sonra buna her bir ihale için teklif verecek her bir yüklenici adayının vereceği cevabı içeren dokümanların boyutu eklenmektedir. Bu dokümanların boyutu da, İdare tarafından hazırlanan dokümanlara verilen cevaplar ve eklenen belgeler dikkate alınarak 12 mb olarak hesaba katılmaktadır. Kamu ihalelerinde teklif veren yüklenici adaylarına ilişkin bir istatistik bulunmamakla birlikte, bu sayının nadiren beşi geçtiği gözlemlenmiştir. Bu nedenle, veri boyutu hesaplanırken bu rakam dikkate alınmış, bu hesaplamalar Çizelge 1.3'te gösterilmiştir.

Çizelge 2.3. Süreç tarafından üretilen/depolanan veri miktarı (Kamu İhale Süreci)

	A	**B**	**C**	**D**	**E**	**F**
	İşlem veri boyutu (byte)	**Saatte işlem sayısı (adet)**	**Günlük işlem veri boyutu (AxBx24)**	**Günlük (mb) [C/(1024x1024)]**	**Aylık (mb) (Dx31)**	**Yıllık (gb) (Dx365/1024)**
Min						
Ort	10 mb + (12 mbx5) = 70 mb	-	-	-	-	70 x 14 = 980 mb
Max						

4. Süreç işlem hızı (mevcut/istenen/max/min) veri temin edilebilmesi halinde mevcut değerler ile geleceğe ilişkin tahminler Çizelge 1.4'e göre doldurulacaktır. Burada ayrıca ağ gecikmesi ya da işlem gecikme toleransı ile birlikte anlık işlem doğrulamanın gerekli olup olmadığı da belirtilecektir.

Çizelge 2.4. Süreç işlem hızı (Kamu İhale Süreci)

İşl. hızı	**Mevcut durum**	**Beklenen durum**	**İşlem gecikme toleransı**	**Anlık işlem doğrulama**
Min	Belirsiz - değişken	Belirsiz - değişken	Belirsiz - değişken	Hayır
Ort	Belirsiz - değişken	Belirsiz - değişken		
Max	Belirsiz - değişken	Belirsiz - değişken		

5. Sürecin özellikleri dikkate alınarak blokzincir üçlü açmazı olarak da bilinen üç niteliğe ilişkin değerlendirme Çizelge 1.5'e göre yapılacaktır. Bu çizelgede, verilen üç özelliğin önem derecesi en önemli 3 olmak üzere belirtilecektir.

EK-2. (devam) Süreç Bilgi Formu (Kamu İhale Süreci)

Çizelge 2.5. Blokzincir üçlü açmazına göre niteliklerin önem dereceleri (Kamu İhale Süreci)

Nitelik	Açıklama	Önem derecesi
Ölçeklenebilirlik	Ölçeklenebilirlik, artan ya da genişleyen iş yükü ya da kapsamına karşılık performans ve verimliliğin korunması demektir. Örnek süreç zamana bağlı olarak kullanıcı sayısı artan bir süreçtir ve gelecekte işlem hacminin artması beklenmektedir. Bu nedenle ölçeklenebilirlik özelliği önem taşımaktadır.	2
Merkezsizlik	Örnek süreç bir kamu kurumu tarafından sunulan bir hizmet olduğundan merkezsizlik gereksinimi nispeten daha az önem taşımaktadır.	1
Güvenlik	İçerdiği veriler ve kullanıcı bilgileri nedeni ile asgari olarak bir veri tabanının sunduğu güvenlik düzeyi beklenmektedir.	3

6. Süreç veri içeriği; sistemde saklanacak olan veri ve metaveriyi tanımlamaktadır. Bu bilgi sürece bağlı olarak her türlü bilgi olabilir. Süreç içerisinde blokzincire kaydedilecek olan veriler, Çizelge 1.6'da verilen şablona uygun biçimde listelenecektir.

Çizelge 2.6. Süreç veri içeriği ve veri sınıfı (Kamu İhale Süreci)

	Veri	Boyut	Açıklama	Veri sınıfı
	Blok #	4 byte	Blok numarası	Herkese açık
	Blok Boyutu	4 byte	Bu alanı takip eden bloğun boyutu	Herkese açık
	Önceki bloğun hash değeri	32 byte	Zincirdeki önceki bloğun (parent) hash referansı	Herkese açık
	Merkle Ağacı	32 byte	Bu bloktaki işlemlerin Merkle ağacının kökünün hash değeri	Herkese açık
	Zaman damgası	4 byte	Bloğun yaklaşık yaratılma zamanı (Unix Epoch saniye)	Herkese açık
	İşlem sayısı	4 byte	Bloğun içerdiği işlemlerin adedi	İzne tabi
Süreç Bilgileri	İhale ilanı	10 – 22 mb	Süreç verileri ve blok yapısına ilişkin detaylar Beşinci Bölümde kapsamlı biçimde verilmiştir.	İzne tabi
	Ön şartlar			İzne tabi
	İdari şartlar ve ekler			İzne tabi
	Teknik şartlar ve ekler			İzne tabi
	Taslak sözleşme			Özel
	İdari şartlara cevaplar			Özel
	Teknik şartlara cevaplar			Özel
	Sözleşme taslağına cevaplar			Özel
	İdareye sorular			İzne tabi
	Yüklenici adayına sorular			Herkese açık

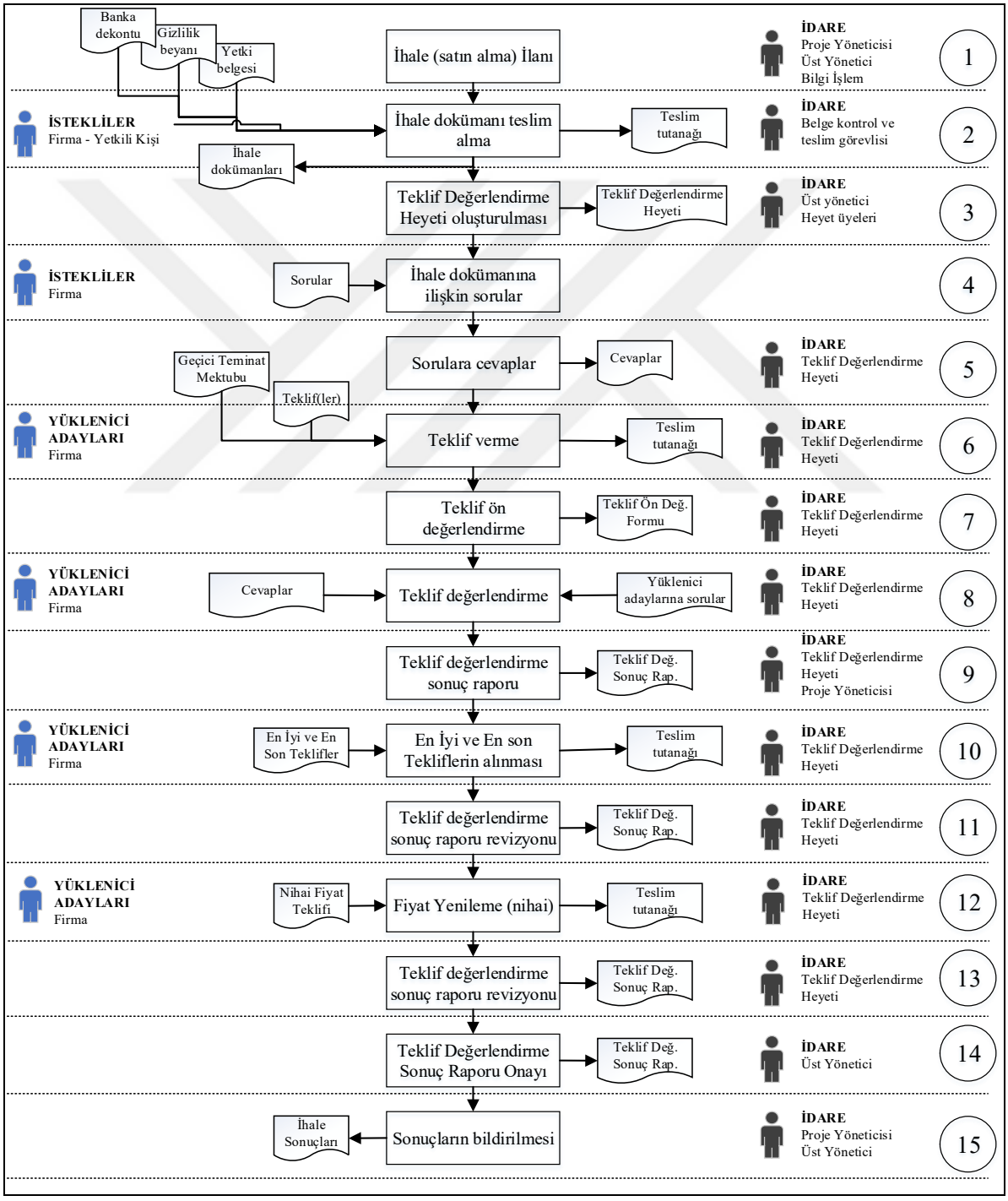
7. Veri sınıflandırma; Süreçte kullanılan, üretilen ve depolanan verilerin sınıflandırılmasına ilişkin bilgileri içermektedir. Buna göre veriler aşağıdaki biçimde sınıflandırılacaktır:

Çizelge 2.6'da verilmiştir.

EK-2. (devam) Süreç Bilgi Formu (Kamu İhale Süreci)

8. Sürecin işleyişi: Süreç tüm faaliyet, alt faaliyet ve alt süreçleri ile birlikte detaylı biçimde tanımlanacaktır. Bu tanımlama işlem adımları ve/veya akış şeması biçiminde olacak, her bir adım birinci maddede listelenmiş olan roller ile ilişkilendirilecektir.

Sürecin işleyişi Şekil 2.1'de verilmiş olan on beş adımdan oluşmaktadır.



Şekil 2.1. Kamu İhale Sürecinin işleyişi

EK-2. (devam) Süreç Bilgi Formu (Kamu İhale Süreci)

9. Hassas, gizli ya da kritik bilgi ya da veri kullanımı; süreç içerisinde kişisel bilgiler, sağlık verileri, gizlilik dereceli veriler gibi hassas veriler kullanılıyorsa belirtilecektir.

Süreç içerisinde hazırlanan ve kullanılan veri ve bilgileri içeren dokümanlar Şekil 2.1'de verilmiş olup bunların gizlilik ya da kritikliklerine ilişkin bilgi Çizelge 2.7'de listelenmiştir:

Çizelge 2.7. Kamu İhale Sürecinde kullanılan veri ve bilgilerin gizlilik dereceleri

Bilgi ve belgeler	Özellik
Banka dekontu	Açık
Gizlilik beyanı	Açık
Yetki belgesi	Kişisel bilgiler içermektedir
İhale dokümanı teslim tutanağı	Kişisel bilgiler içermektedir
İhale dokümanları	Gizli
Teklif Değerlendirme Heyeti Üye Listesi	Gizli
Sorular (isteklilerden)	Gizli
İsteklilerin sorularına cevaplar	Gizli
Geçici Teminat Mektubu	Gizli
Teklifler	Gizli
Teklif teslim tutanakları	Gizli
Teklif Ön Değerlendirme Formu	Gizli
Yüklenici adaylarına sorular	Gizli
Yüklenici adaylarının cevapları	Gizli
Teklif Değerlendirme Sonuç Raporu	Gizli
En İyi ve En Son Teklifler	Gizli
En İyi ve En Son Teklif Teslim Tutanakları	Gizli
Teklif Değerlendirme Sonuç Raporu Rev.1	Gizli
Nihai Fiyat Teklifi	Gizli
Nihai Fiyat Teklifi Teslim Tutanakları	Gizli
Teklif Değerlendirme Sonuç Raporu Rev.2	Gizli
Teklif Değerlendirme Sonuç Raporu Onayı	Gizli
İhale sonuçları ve sözleşmeye davet	Açık

10. Dış bilgi gereksinimi; süreç içerisinde sensör, IoT, elle veri girişi gibi dış veriler kullanılıyorsa bunlar belirtilecektir.

Süreç içerisinde banka dekontu, geçici teminat mektubu, yetki belgesi gibi dış dokümanlar kullanılmakla birlikte bunların tamamı teklif paketi içerisinde değerlendirilmektedir.

11. Mevcut mevzuat; sürece ilişkin varsa yasal düzenlemeler belirtilecektir. Bu yasal düzenlemeler kanun, yönetmelik, yönerge, talimat, standart olabileceği gibi kurum içi düzenleme de olabilecektir. Eğer sürecin işleyişi bir kalite dokümanına dayanıyorsa bu dokümana referans verilecektir.

EK-2. (devam) Süreç Bilgi Formu (Kamu İhale Süreci)

Örnek uygulama için bir kamu kurumunun kalite dokümanlarında tanımlı kurum içi Süreç Tanımı kısmen esas alınmıştır.

12. Fonksiyonel gereksinimler; Bu gereksinimler blokzincire dayalı sistemin gerçekleştirmesi ya da başarması gereken özelliklerdir. Bir başka ifade ile, sistemin vermesi gereken hizmetlerdir ve sistemin ne yapması gerektiğini açıklarlar.

Fonksiyonel gereksinimlere ilişkin değerlendirmeler Çizelge 2.8'de verilmiştir.

Çizelge 2.8. Fonksiyonel gereksinimler (Kamu İhale Süreci)

Gereksinim	**Sürece uygunluk**	**Açıklama**
Ortak ve tutarlı veri saklama	□ Evet	Süreç içerisinde İdare ve Yüklenici adayları tarafından sağlanan verilerin tutarlı bir biçimde saklanması ve ilgilileri ile paylaşılması gerekmektedir.
Birden fazla kullanıcının kayıt yazabilmesi	□ Evet	Süreç içerisinde İdarenin farklı görevlileri ve üst yöneticisi, yüklenici adaylarının görevlendirdiği yetkililer gibi birden fazla sayıda kullanıcının kayıt yapması gerekmektedir.
Tüm kayıt ekleyebilen aktörler arasında güven ve hiyerarşi eksikliği	□ Evet	Birden fazla yüklenici adayı birbirleri ile rakip durumundadır. Ayrıca, İdare yüklenici adaylarına destekleyici kanıtları ölçüsünde güvenmektedir.
Aracı ya da merkezi otorite bulunmaması	□ Evet	Sürecin yönetilmesi için İdare'nin merkezi bir otorite konumunda bulunması gerekmektedir.
Kayıtların değiştirilememesi, silinememesi, güncellenememesi	□ Evet	İhale dokümanları ve teklif paketlerinde sonradan değişiklik yapılmaması esastır.
Katılımcıların belirlenen düzeyde anonimliğe sahip olması	□ Evet	Teklifler değerlendirilirken objektifliğin korunması ve gizliliğin sağlanması için anonimlik özelliğinden faydalanılabilir.

13. Fonksiyonel olmayan gereksinimler; Bu gereksinimler sistemin beklenen özelliklerini tanımlamaktadır. Sistemin kalite özelliklerini tanımlar, sistem kısıtlarını ve olması beklenen durumu tarif ederler. Fonksiyonel olmayan gereksinimler karşılanmadığı takdirde sistem kullanışsız hale gelebilir.

Fonksiyonel olmayan gereksinimlere ilişkin değerlendirmeler Çizelge 2.9'da verilmiştir.

EK-2. (devam) Süreç Bilgi Formu (Kamu İhale Süreci)

Çizelge 2.9. Fonksiyonel olmayan gereksinimler (Kamu İhale Süreci)

Gereksinim	Süreç için kritiklik	Açıklama
Ölçeklenebilirlik	□ Düşük	İşlem adedi yıl içinde gerçekleştirilebilecek ihale sayısının az olması nedeniyle düşüktür.
İşlem hızı	□ Düşük	İhale değerlendirme sürecinin belirli bir zamana yayılması nedeniyle işlem hızı öncelikli bir kriter değildir.
İşlem hacmi	□ Düşük	Yıl içinde gerçekleştirilebilecek ihale sayısının sınırlı olması nedeniyle düşüktür.
Sistem güvenliği (çatallanma, mutabakat mekanizması açıkları)	□ Yüksek	İçerdiği gizli ve hassas bilgiler nedeniyle güvenlik gereksinimi yüksektir.
Diğer sistemlerle entegrasyon	□ Orta	Tekliflerin hazırlanması, sözleşme yönetimi, muhasebe gibi sistemlerle entegrasyon şart olmamakla birlikte verimliliği artıracağı değerlendirilmektedir.
Verimlilik	□ Orta	Elden doküman teslimi, basılı evrak üzerinden değerlendirme gibi manuel adımların dijitalleşmesi imkânı ile kontrol ve onay adımlarının blokzincir tasarımı ile dijital olarak yürütülebilmesi imkanının verimliliği artıracağı değerlendirilmektedir.
Mevzuat düzenlemelerine uyum	□ Yüksek	Mevzuata uyum mutlaka sağlanması gereken özelliktir.
Teknik ve süreç olgunluk/ standardizasyon düzeyi	□ Orta	-
Şeffaflık	□ Yüksek	Hesap verebilirlik ve objektiflik bakımından sürecin sonuçlarının gizli bilgiler gözetilerek şeffaf olması yüksek önemdedir.

14. Mevcut süreç/faaliyetle ilgili problemler ya da iyileştirilebilir noktalar; blokzincir çözümünün uygulanacağı sürecin mevcut durumundaki problemler, darboğazlar ve iyileştirilebilir alanlar bu kısımda, aşağıdaki tablo kullanılarak listelenecektir. Tabloda örnek olarak bazı durumlar verilmiştir.

Mevcut sürece ilişkin problemler ve iyileştirilebilir noktalara ilişkin değerlendirmeler Çizelge 2.10'da verilmiştir.

EK-2. (devam) Süreç Bilgi Formu (Kamu İhale Süreci)

Çizelge 2.10. Fonksiyonel olmayan gereksinimler (Kamu İhale Süreci)

Mevcut problem-darboğaz-iyileştirilebilir alan	**Tipi (Problem, iyileştirilebilir alan)**	**Blokzincirden faydalanılabilir mi?**
Gizlilik ve güvenlik: ihale dokümanlarının içerebileceği gizlilik dereceli bilgilerin yüklenici adayları dışında erişilememesi istenebilir. Ayrıca, yüklenici adaylarının fiyat tekliflerinin teknik değerlendirme tamamlanmadan heyet üyelerince bilinmemesi, yine bu fiyat tekliflerinin açıldıktan sonra da heyet üyeleri dışındaki herhangi bir tarafla paylaşılmaması gerekmektedir. Bu kontroller gizlilik beyanı, teslim tutanakları, fiyat açma işleminin tutanak altına alınması gibi manuel işlemleri içermektedir.	□ İyileştirilebilir alan	□ Evet
Erişim kontrolleri: ihale dokümanlarına hem fiziki hem de dijital ortamda sadece yetkilendirilmiş taraflar erişebilmeli, teklifler alındıktan sonra herhangi bir değişiklik yapılmaması garanti edilmelidir. Erişimlerin yetkililer dışında engellenmesinin yanı sıra dokümanlara kimlerin, ne zaman eriştikleri de kayıt altına alınmalıdır.	□ İyileştirilebilir alan	□ Evet
Şeffaflık: İhalenin ilanı, tekliflerin alınması, değerlendirilmesi ve açıklanması aşamalarındaki tüm faaliyetlerin şeffaf bir biçimde yürütülmesi esastır. Ancak bu şeffaflık gizlilik ve güvenlik ilkelerini ihlal etmemelidir.	□ İyileştirilebilir alan	□ Evet
Zaman: İhale ilanının yayımlanması, isteklilerin sorularının alınması ve cevaplandırılması, tekliflerin sunulması, yüklenici adaylarına soruların yöneltilmesi ve cevapların alınması, heyet faaliyetleri, değerlendirme sonuçlarının raporlanması gibi işlemler genellikle resmi evraklar aracılığı ile, basılı kağıt ortamında yürütülmekte, evrakların iletilmesi ve işleme alınması için belirli bir zaman harcanmaktadır.	□ İyileştirilebilir alan	□ Evet
Tarih kontrolü: İhale ilanında belirtilen tarih ve saatten sonra teklif verilmesi halinde bu teklif değerlendirmeye alınmamaktadır. Tekliflerin teslim zamanının kontrolü manuel olarak yapılmaktadır.	□ İyileştirilebilir alan	□ Evet



GAZİLİ OLMAK AYRICALIKTIR.