
GAZİ ÜNİVERSİTESİ
Gazi
1926

BLOKZİNCİR TABANLI DİJİTAL KİMLİK İLE ELEKTRONİK TİCARETTE GÜVENİN ARTIRILMASI

Ömer DOĞAN

DOKTORA TEZİ
YÖNETİM BİLİŞİM SİSTEMLERİ ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

HAZİRAN 2023

ÖMER DOĞAN tarafından hazırlanan "BLOKZİNCİR TABANLI DİJİTAL KİMLİK İLE ELEKTRONİK TİCARETTE GÜVENİN ARTIRILMASI" 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. Hacer KARACAN

Bilgisayar Mühendisliği, Gazi Üniversitesi

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

Başkan: Prof. Dr. Bilal TOKLU

Endüstri Mühendisliği, Gazi Üniversitesi

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

Üye: Prof. Dr. Süleyman ERSÖZ

Endüstri Mühendisliği, Kırıkkale Üniversitesi

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

Üye: Prof. Dr. M. Ali AKCAYOL

Bilgisayar Mühendisliği, Gazi Üniversitesi

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

Üye: Doç. Dr. Mehmet ŞİMŞEK

Bilgisayar Mühendisliği, Millî Savunma Üniversitesi

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

Tez Savunma Tarihi: 15/06/2023

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.

Ömer DOĞAN

15/06/2023

BLOKZİNCİR TABANLI DİJİTAL KİMLİK İLE ELEKTRONİK TİCARETTE GÜVENİN ARTIRILMASI

(Doktora Tezi)

Ömer DOĞAN

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Haziran 2023

ÖZET

E-ticaret işlemlerinde, satıcıların sunduğu ticari kimlikler, sertifikalar ve akreditasyon belgeleri gibi belgelerin doğruluğunun kanıtlanması geleneksel yöntemlerle mümkün değildir. Çünkü dijital ortamda sunulan bu belgeler, aslında kâğıt ortamındaki karşılıklarının dijital ortama aktarılmış halidir ve bunlar kolayca taklit edilebilir. Bu nedenle, yetkili kuruluşların bu belgeleri satıcılara doğrudan dijital olarak sunabileceği ve alıcıların bu belgeleri güvenilir bir şekilde doğrulayabileceği bir yapıya ihtiyaç vardır. Bu şekilde oluşturulacak bir yapı ile e-ticarette karşılaşılan güven sorunlarının büyük bir kısmının çözülmesi mümkündür. Bu çalışmada, genel olarak dijital kimlik olarak adlandırılan bu belgelerin yetkili kuruluşlar tarafından güvenli bir şekilde verilmesi ve alıcılar tarafından doğrulanması amacıyla blok zinciri tabanlı bir dijital kimlik güven çerçevesi önerilmektedir. E-ticaret işlemlerinde güvenin sağlanmasındaki bir başka unsur da alıcıların satıcılar hakkında yaptığı değerlendirmeler ve satıcıların itibar puanlarıdır. Alıcıların gönderdiği geri bildirimler, diğer potansiyel alıcıların satın alma kararlarında önemli bir rol oynamaktadır. Bu çalışmada, dijital kimlik güven çerçevesi ile oluşturulan blok zinciri alt yapısı genişletilerek e-ticaret itibar sistemi için de kullanılmaktadır. Önerilen itibar değerlendirme sistemi, bilinen bazı saldırılara karşı önlemler içeren gizlilik korumalı blok zinciri tabanlı ve merkezi olmayan bir itibar sistemidir. Sistem, Hyperledger Indy ve Hyperledger Fabric olmak üzere iki farklı özel blok zinciri üzerine kurulmuştur. Sistem, yetkili kuruluşların e-ticaret firmalarına dijital kimlik sağlaması ve itibar sistemi içerisinde dijital kimlik biçiminde geri bildirim jetonu ve indirim jetonu verilmesi ile güvenli bir mekanizma sağlanmaktadır. Sonuç olarak, bu önerilen yaklaşım ile blok zinciri teknolojisi ve dijital kimlikler kullanılarak e-ticarette güvenin artırılması hedeflenmektedir.

Bilim Kodu	:	114604
Anahtar Kelimeler	:	E-Ticaret, İtibar Sistemi, Dijital Kimlik, Doğrulanabilir Kimlikler, Blok Zinciri, Güven Çerçevesi
Sayfa Adedi	:	94
Danışman	:	Prof. Dr. Hacer KARACAN

BUILDING TRUST IN ELECTRONIC COMMERCE USING BLOCKCHAIN BASED DIGITAL IDENTITY

(Ph. D. Thesis)

Ömer DOĞAN

GAZİ UNIVERSITY

INSTITUTE OF INFORMATICS

June 2023

ABSTRACT

In e-commerce activities, the validation of the seller records, such as commercial identity, licenses, accreditation certificates, quality certificates and other kinds, is not possible by using traditional ways. This is because the digitally presented records are simply the images of their physical counterparts in paper and these images can easily be fabricated. Therefore, a mechanism is needed in the digital world that allows authorized organizations to issue digital records and buyers to validate them digitally in a trusted way. With such a mechanism established, it would be possible to overcome most of the issues related with trust in e-commerce. This study proposes a blockchain based digital identity trust framework that allows authorities to issue digital identities and buyers to verify them in a secure way. Other factors for building trust in e-commerce are the feedback provided by the buyers about the sellers and the reputation scores of the sellers. Buyer feedbacks play an important role in the decision of prospective buyers about involving in an e-commerce transaction with the sellers. With this study, the blockchain infrastructure established by the proposed trust framework is extended to be used in a new e-commerce reputation system. The e-commerce reputation system proposed in this study is a privacy preserving blockchain based and decentralized reputation system that has counter measures against some known attacks. The whole system is built on top of two private blockchains, namely Hyperledger Indy and Hyperledger Fabric. The system allows the authorities to issue digital identities to sellers and provides a secure mechanism within the reputation system for issuance and verification of feedback tokens and discount tokens in the form of digital identities. As a result, it is aimed to build trust in e-commerce using blockchain technology and digital identities with the proposed approach.

Science Code	:	114604
Key Words	:	E-Commerce, Reputation System, Digital Identity, Verifiable Credentials, Blockchain, Trust Framework
Page Number	:	94
Supervisor	:	Prof. Dr. Hacer KARACAN

TEŞEKKÜR

Bu tezi tamamlama yolculuğunda bana destek olan herkese içtenlikle teşekkürlerimi sunarım.

Öncelikle, danışman hocam Prof. Dr. Hacer KARACAN'a, bilgi birikimi, sabrı, rehberliği ve teşvik edici tutumu için içtenlikle teşekkür etmek isterim. Doktora çalışmalarımın başından sonuna kadar bu zorlu süreçte ilerlememi sağlayan motive edici ve yol gösterici yaklaşımından ve desteklerinden dolayı sonsuz teşekkürler. Danışmanım olduğunuz için daima gurur duyacağım.

Tez çalışmamım niteliğini artırmada önemli bir rol oynayan tez izleme komitesinin değerli üyeleri Prof. Dr. M. Ali AKCAYOL ve Prof. Dr. Süleyman ERSÖZ hocalarıma, değerli görüşleri, yapıcı eleştirileri ve önerileri için çok teşekkür ederim.

Bu çalışma süresince yanımda olan ve bana her zaman destek olan kıymetli eşim Hülya DOĞAN'a ve oğlum Kerem DOĞAN'a, gösterdikleri sabır ve anlayış için çok teşekkür ederim. Bu süreçteki en büyük destekçim ve motivasyon kaynağım oldukları için sonsuz teşekkürler.

İÇİNDEKİLER

Sayfa

ÖZET iv

ABSTRACT v

TEŞEKKÜR vi

İÇİNDEKİLER vii

ÇİZELGELERİN LİSTESİ x

ŞEKİLLERİN LİSTESİ xi

SİMGELER VE KISALTMALAR xii

1. GİRİŞ 1

2. KAVRAMSAL ÇERÇEVE 7

2.1. Dijital Kimlikler 7

2.2. Doğrulanabilir Kimlikler 8

2.3. Blok Zinciri 8

2.4. Akıllı Sözleşmeler 10

2.5. Hyperledger 11

2.6. Sıfır Bilgi İspatı 12

3. LİTERATÜR ARAŞTIRMASI 13

3.1. Dijital Kimlik Güven Çerçevesi 13

3.2. İtibar Sistemi 17

3.2.1. Açık blok zincirler üzerine geliştirilen e-ticaret itibar sistemleri 17

3.2.2. Özel blok zincirler üzerine geliştirilen e-ticaret itibar sistemleri 19

3.2.3. Açık blok zincirler üzerine geliştirilen diğer itibar sistemleri 20

3.2.4. İtibar sistemleri üzerine literatür taramaları 21

3.2.5. Merkezi defter veri tabanları 22

Sayfa

4. E-TİCARET DİJİTAL KİMLİK GÜVEN ÇERÇEVESİ 23
4.1. İlkeler 23
4.2. Dijital Kimlik Yönetim Şeması 24
4.3. Dijital Kimlik Veri Yapısı 26
4.4. Güven Çerçevesi Rolleri 27
4.5. Dijital Kimlik Çeşitleri 29
4.5.1. Temel dijital kimlikler 30
4.5.2. Bağlamsal dijital kimlikler 33
4.6. Kimlik İspatı ve Dijital Kimlik Alma 36
4.7. Dijital Kimlik İbrazı ve Doğrulama 40
4.8. Güven İşareti 42
4.9. Güven Çerçevesi Paydaşları ve Yönetişimi 43
5. BLOK ZİNCİRİ TEMELLİ E-TİCARET İTİBAR SİSTEMİ 49
5.1. Modelin Prensipleri 49
5.2. Model Mimarisi 50
5.2.1. Doğrulanabilir kimlik alt sistemi 51
5.2.2. Geri bildirim toplama alt sistemi 54
5.3. Süreçler 58
5.3.1. Satıcı kayıt fazı 58
5.3.2. Alışveriş fazı 60
5.3.3. Hizmet sunumu fazı 61
5.3.4. Geri bildirim fazı 61
5.4. İtibar Puanı ve İndirim Jetonu Tutarı Hesaplama 63
5.5. Modelin Güvenliği 67
5.5.1. Mahremiyetin korunması 67
5.5.2. X.509 sertifikaları ile karşılaştırma 69

Sayfa

5.5.3. Güvenlik analizi 70

5.6. Modelin Performansı 73

6. SONUÇ VE ÖNERİLER 79

KAYNAKLAR 85

ÖZGEÇMİŞ 93

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

Çizelge 3.1. Blok zinciri tabanlı itibar sistemleri 20
Çizelge 4.1. Temel dijital kimlikler 30
Çizelge 4.2. E-ticaret işlemlerine ilişkin örnek bağlamsal dijital kimlikler 35
Çizelge 5.1. Doğrulanabilir kimlik mesaj alışverişleri 75
Çizelge 5.2. Satıcı kayıt fazı metrikleri 75
Çizelge 5.3. Satıcı geri bildirimlerini çekme yanıt süreleri 76
Çizelge 5.4. Geri bildirim fazı metrikleri..... 77
Çizelge 5.5. Kanıtın doğrulanması, geri bildirimin blok zincirine eklenmesi ve itibar puanının hesaplanması 77

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil 2.1. Blok zinciri 9
Şekil 4.1. Doğrulanabilir kimlik rolleri ve veri akışı 26
Şekil 4.2. E-ticaret dijital kimlik güven çerçevesi rolleri 29
Şekil 4.3. E-ticaret işlemlerine ilişkin örnek bağlamsal dijital kimlikler 34
Şekil 4.4. EKDS kimlik doğrulama örnek süreci 39
Şekil 4.5. EKDS doğrulaması ile dijital kimlik alma 40
Şekil 4.6. Güven damgası 43
Şekil 4.7. Blok zinciri tabanlı dijital kimlik mimarisi 45
Şekil 5.1. GTS mantıksal veri modeli 55
Şekil 5.2. Genel sistem ağ mimarisi 57
Şekil 5.3. Satıcı kaydı sıralama diyagramı 60
Şekil 5.4. Hizmet sunumu fazı sıralama diyagramı 63
Şekil 5.5. Her bir adımın ortalama gecikme süresi 78

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler	**Açıklamalar**
ms	Milisaniye
B	Bayt
KB	Kilo Bayt
MB	Mega Bayt

Kısaltmalar	**Açıklamalar**
BCTR	Blockchain Türkiye Platformu
BM	Birleşmiş Milletler
DB	Dünya Bankası
DEF	Dünya Ekonomik Forumu
DIACC	Digital Identification and Authentication Council of Canada
E-ticaret	Elektronik Ticaret
EKDS	Elektronik Kimlik Doğrulama Sistemi
ID4D	Identification for Development
ISO	International Organization for Standardization
ITU	International Telecommunication Union
KEC	Kart Erişim Cihazı
KDPS	Kimlik Doğrulama Politika Sunucusu
KVKK	Kişisel Verileri Koruma Kanunu
LTS	Long-Term Support
MERSİS	Merkezi Sicil Kayıt Sistemi
NIST	National Institute of Standards and Technology
NVİGM	Nüfus ve Vatandaşlık İşleri Genel Müdürlüğünde

OITF	Open Identity Trust Framework
P2P	Peer to Peer
PCTF	Pan-Canadian Trust Framework
PoS	Proof of Stake
PoW	Proof of Work
RAM	Random Access Memory
TOBB	Türkiye Odalar ve Borsalar Birliği
TOIP	Trust Over IP
TSE	Türk Standartları Enstitüsü
TÜRKAK	Türk Akreditasyon Kurumu
UEKAE	Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
USB	Universal Serial Bus
vCPU	Virtual Central Processing Unit
W3C	World Wide Web Consortium
ZKP	Zero Knowledge Proof

1. GİRİŞ

E-ticaretin hem Türkiye'deki hem de global alandaki büyüme hızı gözle görülür bir şekilde artmaktadır. Dünya genelindeki perakende e-ticaret satışları son beş yıl içerisinde 107% oranında bir artış kaydetmiştir (Statista, 2022). Ancak, e-ticaret ekosisteminde yer alan satıcı firmaların sundukları bilgilerin doğruluk payının belirsizliği, potansiyel alıcıların e-ticaret alışverişlerinde güvensizlik hissetmelerine yol açmaktadır. Çevrimiçi işlemlerde sıkça rastlanan bir durum olan, kullanıcıların karşı tarafın kimlik bilgilerini doğru bir şekilde bilememe ya da bu bilgilerin doğruluğundan emin olamama sorunları, e-ticaret işlemlerinde de yaşanmaktadır. Satıcıların, ticari kimliklerine ve sertifika, akreditasyon belgesi, izin belgesi, kalite belgesi gibi diğer belgelere dair çevrimiçi olarak sundukları bilgiler genellikle fiziksel belgelerin dijital hale getirilmiş görselleri olduğu için, bu bilgilerin doğruluğunun ispatlanması ve yetkili bir kuruluş tarafından onaylanması çoğunlukla mümkün olmamaktadır. Bu sebeple, satıcıların bu bilgileri ve belgeleri dijital olarak yetkili kurumlarca alabileceği, gerektiğinde dijital bir şekilde sunabileceği ve alıcılara bu bilgilerin ve belgelerin doğruluğunu kanıtlayabileceği bir sistem oluşturulmasına ihtiyaç duyulmaktadır.

Satıcı firmaların bilgi ve belgelerini ispatlamalarının yanı sıra, alıcının satıcıya güven duymasını ve satıcı ile bir alışveriş ilişkisine girme kararını etkileyen birçok faktör vardır. Bu faktörlerden biri olan satıcının itibarı, alıcıların satın alma deneyimleri sonucunda verdikleri geri bildirimler, yorumlar ve değerlendirmeler aracılığıyla birikimli olarak oluşur. Zaman içinde oluşan satıcı itibarı, olası alıcıların bir satıcıyla e-ticaret işlemine girip girmeme kararını vermelerine yardımcı olur. Bu tür geçişken güven, Kamvar, Schlosser ve Garcia-Molina (2003) tarafından P2P ağlarda itibar yönetimi için EigenTrust algoritması olarak formüle edilmiştir. Birçok e-ticaret sitesi, alışverişi tamamladıktan sonra alıcıların satıcılar için yorum ve puan göndermesine olanak sağlar. Bu yorum ve puanlar, e-ticaret sitesinin itibar sistemi tarafından toplanır, işlenir ve her bir satıcı için bir itibar puanı hesaplanır. Bu yorumlar ve itibar puanları, alıcıların satıcıları tanımasa da satıcılara karşı bir dereceye kadar güven duymasını sağlar. Ancak, itibar sistemlerine karşı güvenilirliği azaltabilecek birçok olası veya karşılaşılmış olan saldırı türü vardır. Koutrouli ve Tsalgatidou (2012) bu saldırılar hakkında kapsamlı bir inceleme yapmışlar ve saldırıların bir taksonomisini oluşturmuşlardır. Bu taksonomi, adil olmayan (taraflı) tavsiyeler, tutarsız davranışlar ve kimlik yönetimi ile ilgili saldırılar olmak üzere üç ana kategori içerir. Bu

saldırı türlerinden alıcıların satıcılar için geri bildirim gönderdiği bir e-ticaret itibar sistemi için geçerli olan saldırılar aşağıda listelenmiştir.

Kötüleme saldırısı, bir saldırganın satıcıların itibarını düşürmek için yanlış olumsuz geri bildirim verdiği "adil olmayan (taraflı) tavsiye" saldırı türlerinden biridir. Bu saldırı genellikle bir satıcının rakipleri tarafından gerçekleştirilir.

Sahte Oylama saldırısı, kötüleme saldırısının tam tersidir. Bu saldırıda amaç, sisteme yanlış olumlu geri bildirimler enjekte ederek bir satıcının itibar puanını artırmaktır. Hasan ve arkadaşları tarafından belirtildiği gibi, bu saldırı genellikle iki kullanıcı tarafından karşılıklı olarak gerçekleştirilir. Her iki kullanıcı da sürekli olarak birbirleriyle işlem yaparlar ve daha sonra birbirlerine olumlu geri bildirim verirler.

Aklama/Yeniden Giriş saldırısı, kimlik yönetimi ile ilgili bir saldırıdır. Kötü bir itibara sahip olan bir satıcı, sistemden çıkar ve daha sonra sıfır bir itibarla sisteme yeniden katılır. İtibar sisteminde eski satıcı kimliği ile yeni kimliği ilişkilendirmek için bir yol yoksa sistem bu tür saldırılara açıktır.

Sybil saldırısı, saldırganın itibar puanları üzerinde daha fazla etkiye sahip olmak için sistemde birden fazla kimlik oluşturmasıyla gerçekleştirilir. Birden fazla kimliği olan saldırgan, bu avantajı hem kötüleme hem de sahte oylama amaçlı kullanabilir. Bir itibar sisteminin Sybil saldırısına karşı zafiyeti, kimliklerin ne kadar kolay bir şekilde oluşturulabileceğine, itibar sisteminin güven zinciri ile güvenilir bir varlığa bağlantısı olmayan varlıklara güvenip güvenmediğine ve itibar sisteminin tüm varlıklara eşit şekilde davranıp davranmadığına bağlıdır.

İhanet saldırısı, saldırganın güvenilir görünmek için bir süre düzgün davrandığı ve daha sonra aldatmaya başladığı saldırı türüdür. Bu saldırı türüne internet üzerindeki en büyük açık artırma usulü alışveriş sitesi olan eBay'de karşılaşılmıştır. Bu durumda, satıcılar küçük meblağlı birçok işleme katılarak bir süre güven oluşturmuşlardır. Daha sonra ise yüksek fiyatlı ürünlerle yapılan işlemlerde alıcıları kandırmışlardır.

Geleneksel e-ticaret sistemlerinde, itibar genellikle alıcıların satıcılar hakkında verdikleri yorum ve puanları merkezi bir şekilde toplayan ve depolayan platformlar tarafından

yönetilir. Merkezi itibar sistemlerinin, veri manipülasyonu zafiyeti, şeffaf olmama ve itibar verilerini birden çok platformda paylaşılmasının zor olması gibi çeşitli sınırlamaları vardır. Blok zinciri teknolojisi, şeffaf, değişmez ve birden çok platformda paylaşılabilen itibar verilerini yönetmenin merkezi olmayan ve değiştirilmeye karşı korumalı bir yöntemini sunar. Bu yöntem ile satıcılar, birden çok e-ticaret platformunda kullanılabilecek güvenilir bir itibar profili oluşturabilir. Öte yandan, blok zinciri tabanlı olmayan itibar sistemleri genellikle merkezi sistemlerdir. Bu sistemlerde itibar verileri, tek bir e-ticaret platformu tarafından kontrol edildiğinden manipülasyona ve sansüre karşı zafiyet barındırmaktadır.

Bu tez çalışması kapsamında blok zinciri tabanlı merkezi olmayan ve dijital kimlikleri kullanan bir itibar sistemi modellenerek itibar sistemlerine yönelik bilinen saldırılara karşı önlemler oluşturulmuştur. Ayrıca dijital kimliklerin e-ticaret ekosisteminde yer alan satıcı, üretici firma, pazar yeri gibi paydaşlar tarafından kullanımları ve bu paydaşların paylaşmak istedikleri bilgi ve belgeleri dijital kimlikler aracılığıyla güvenli bir şekilde çevrim içi olarak sunabilmeleri hedeflenmiştir. Yetkili kuruluşlar tarafından firmalara verilen bu belgelerin yine yetkili kuruluşların da sürecin içinde bulunduğu yöntemlerle doğru, geçerli ve değiştirilmemiş belgeler olduğunun çevrim içi olarak kanıtlanabilmesine yönelik bir öneri sunulmuştur. Dijital kimliklerin e-ticarette belirtilen yöntemlerle kapsamlı kullanılması durumunda, e-ticaretin bir diğer paydaşı olan alıcıların satın alma işlemlerini yaparken sisteme daha fazla güven duymasını sağlayabilir. Ancak, alıcıların sisteme olan güvenlerini artırabilmek için, e-ticaret ekosistemindeki işlemlerin belirlenen kurallar dahilinde açık bir biçimde yürütülmesi, işlemlerde rol alan paydaşların belirli kurallara uygun bir biçimde hareket etmeleri ve sistemin siber güvenlik alt yapısının siber ataklara karşı yeterli seviyede koruma sağlayan bir güvenlik seviyesi sunması gerekmektedir. Tüm bu süreçleri ve kuralları düzenleyen dijital kimlik güven çerçevesi, dijital kimliklerin verilmesinden başlayarak tüm dijital kimlik yaşam döngüsüne ilişkin işlemlerin güvenilir bir şekilde gerçekleştirilmesini amaçlayan tanımlamaları, ilkeleri, uyumluluk ölçütlerini, değerlendirme metodolojilerini, standartları ve koşulları içeren bir kurallar bütünüdür (The Digital Identification and Authentication Council of Canada [DIACC], 2020). Bu tez çalışmasında, dijital kimlik güven çerçevesinin elektronik ticaret alanında kullanılmasına yönelik olarak bu alanda detaylı inceleme yapılmış ve elektronik ticaret alanına özel olarak bir dijital kimlik güven çerçevesi oluşturulmuştur. Elektronik ticarete özel dijital kimlik güven çerçevesi, blok zinciri alt yapısına sahip ve paydaşlardan yalnızca firmaların dijital kimlik sahibi olduğu bir

kapsamda ele alınmıştır. Elektronik ticaret paydaşlarından alıcıların dijital kimlik sahibi olması durumu bu tez kapsamında ele alınmamıştır.

Blockchain Türkiye Platformu (BCTR) tarafından hazırlanan Dijital Kimlik Raporu'na göre, kimlik; "kişiye ait biyografik ve biyolojik özellikler de dâhil olmak üzere, bir kişiyi tekil olarak betimleyen özellikler ve karakteristik davranışlar" olarak ifade edilmiştir (BCTR, 2019). Ancak bu çalışmada, kimlik sadece bireylerle sınırlı tutulmamış, her tür varlık için geçerli kabul edilmiştir. Uluslararası Telekomünikasyon Birliği (ITU) tarafından yapılan kimlik tanımı; "varlıkların bağlam içinde belirgin bir şekilde ayrıştırılmasını sağlayan bir ya da daha çok özelliklerin temsili" şeklinde ifade edilmiştir (ITU, 2018). Bu tanım, şirketlerin de içerisinde olduğu geniş kapsamlı bir kimlik tanımıdır. Varlıkları birbirinden ayıran özellikler, varlığın türüne göre değişkenlik gösterebilir. Bireyleri ayırt eden özellikler kimlik numarası, isim, soy isim, biyometrik veriler gibi kişiye özel bilgilerdir. Bunun yanı sıra firmalar için ise ticari sicil numarası, vergi numarası, MERSİS numarası, işletme adı, adres, kurulduğu tarih ve belgelendirme gibi bilgiler ayırt edici olabilir. Bu tanıma dayanarak dijital kimlik, varlıkları tanımlayan, diğer varlıklara göre ayırt edici olan, varlığın öz niteliklerini içeren ve varlığı dijital olarak yansıtan bir unsurdur. Her türlü kimliğin tanımlanmasından başlayan yaşam döngüsünde, kimlik sahibine verilmesi, geçerliliğinin kanıtlanması, kullanılması ve sonlanması gibi aşamalar bulunmaktadır. Dijital kimlikler için de tüm bu aşamalar geçerlidir ve çevrim içi olarak gerçekleştirilir.

Tezin organizasyonu

Tez giriş bölümü dahil toplam 6 bölümden oluşmaktadır. Tezin giriş bölümünde tezin kapsamı, gerçekleştirilen çalışmalar, sağlanan katkılar ve tezin organizasyonu sunulmuştur.

Tezin ikinci bölümünde tez çalışmasına temel teşkil eden kavramlar ve teknolojilerle ilgili arka plan bilgileri verilmiştir. Bu kapsamda dijital kimlikler, doğrulanabilir kimlikler, blok zinciri teknolojisi, akıllı sözleşmeler, bir blok zinciri açık kaynak ürün ailesi olan Hyperledger ve sıfır bilgi ispatı kavramı ve tekniği açıklanmıştır. Bu kavram, teknik ve teknolojiler, tez çalışmasında önerilen model ve sistemlerde kullanılan temel öğelerdir.

Tezin üçüncü bölümünde dijital kimlik güven çerçevesi ve itibar sistemi konularına ilişkin literatür araştırmalarına yer verilmiştir. Dijital kimlik güven çerçevesi ile ilgili olarak farklı

ülkelerin yaptığı çalışmalar ile ülkelerden bağımsız organizasyonların gerçekleştirdiği çalışmalar ayrı ayrı ele alınmıştır. İtibar sistemi konusunda yapılan çalışmalar ise alt başlıklar halinde gruplanarak verilmiştir. Öncelikle açık ve özel blok zincirler üzerine geliştirilen e-ticaret itibar sistemlerine ilişkin çalışmalar ayrı ayrı verilmiştir. Daha sonra literatürde yer alan, açık blok zincirler üzerine e-ticaret dışı sektörler için geliştirilen itibar sistemlerine yer verilmiştir. İtibar sistemlerine ilişkin literatür taramaları ayrı bir başlık altında sunulmuştur. Ayrıca, özel blok zincirlere alternatif olarak değerlendirilebilecek merkezi defter veri tabanı teknolojine ilişkin literatürdeki çalışmalara yer verilerek tez çalışmamızdaki itibar sisteminin bu açıdan değerlendirmesi yapılmıştır.

Tezin dördüncü bölümünde bu çalışma kapsamında önerilen e-ticaret dijital kimlik güven çerçevesi modelinin detaylarına yer verilmiştir. Bu kapsamda öncelikle dijital kimlik güven çerçevesinin hangi prensipler üzerine kurulduğu açıklanmıştır. Daha sonraki alt bölümlerde ise bu prensipleri karşılayan güven çerçevesi öğeleri verilmiş ve bu öğeler için modelimizde çözüm önerileri sunulmuştur. E-ticaret dijital kimlik güven çerçevesinin kimlik yönetim şeması, kimlik veri yapısı, güven çerçevesinde yer alan roller, dijital kimlik çeşitleri, kimlik ispatı ve dijital kimliğin verilmesi süreçleri, dijital kimliğin ibrazı ve geçerliliğinin doğrulanması süreçleri, güven işareti kavramı, güven çerçevesinde yer alan paydaşlar ve güven çerçevesinin yönetimi, denetimi ve kontrolü konuları alt başlıklar halinde detaylı olarak açıklanmıştır.

Beşinci bölümde bu tez çalışması kapsamında önerilen blok zinciri temelli e-ticaret itibar sistemi ayrıntılarıyla açıklanmıştır. Öncelikle önerilen itibar sisteminin temel aldığı prensipler açıklanmıştır. Daha sonra sistemi oluşturan alt sistemler ile birlikte sistem mimarisi anlatılmıştır. E-ticaret işlemleri sırasında gerçekleşen süreçler ve bu süreçlerde itibar sistemimizin nasıl yer aldığı açıklanmıştır. Ayrıca itibar sisteminin önemli bir parçası olan itibar puanı ve indirim jetonuna ilişkin hesaplama algoritmalarına yer verilmiştir. Son olarak önerilen itibar sistemi güvenlik ve performans bakış açısıyla ele alınmış ve sistemin bu bakımlardan analizi ve değerlendirmesi yapılmıştır.

Tezin son bölümü sonuç ve öneriler bölümüdür. Bu bölümde tezin amacı ve gerçekleştirilen çalışmalar kısaca özetlenmiş, yorumlanmış ve tezin literatüre katkıları özet olarak açıklanmıştır. Ayrıca gelecek çalışmalara ışık tutması bakımından yapılabilecek çalışmalara değinilmiştir.

2. KAVRAMSAL ÇERÇEVE

Bu bölümde tez çalışması kapsamında ele alınan kavramsal temeller açıklanmıştır. Farklı anlamlarda kullanılabilen dijital kimlik kavramının bu tez çalışması kapsamındaki kullanımı açıklanmıştır. Dijital kimliklere benzer bir kavram olan doğrulanabilir kimlikler ve bu kavrama temel teşkil eden uluslararası standartlar hakkında bilgi verilmiştir. Tez çalışmasının temel teknolojik alt yapısını oluşturan blok zinciri teknolojisi hakkında temel bilgi verilmiş ve bu teknolojinin getirdiği akıllı sözleşme kavramı ve kullanım amacı açıklanmıştır. Blok zinciri teknolojisinin kurumsal uygulamalara uygulanmasına olanak sağlayan Hyperledger Fabric ve dijital kimlikler için özelleştirilmiş bir blok zinciri alt yapısı olan Hyperledger Indy açık kaynak alt yapıları hakkında bilgi verilmiştir. Ayrıca, tez çalışmasına güvenlik boyutunda katkı sağlayan sıfır bilgi ispatı kavramı açıklanmıştır.

2.1. Dijital Kimlikler

Geleneksel kimlik yönetimi sistemleri, belge tabanlı ve merkezi otoriteler tarafından kontrol edilmektedir. Bu yapılar, sahtecilik, hırsızlık ve gizlilik ihlalleri gibi sorunlara maruz kalmaktadır. Dijital kimlikler, kimlik yönetimi için daha güvenli, şeffaf ve kullanıcı dostu bir alternatif sunar. Dijital kimlik, bir bireyin veya kurumun dijital ortamda temsil edilen kimlik bilgileridir. Dijital kimlikler, kullanıcıların güvenli ve gizli bir şekilde kimliklerini doğrulamalarını ve dijital hizmetlere erişimlerini sağlar. Dijital kimlikler, doğrulanabilir kimlik bilgileri ve kriptografik yöntemler kullanarak, güvenli ve özelleştirilebilir kimlik yönetimi sunar.

Dijital Kimlikler geleneksel kimlik yönetimi yöntemlerine göre birtakım avantajlar sunarlar. Kriptografik yöntemler kullanarak güvenli hale getirilen dijital kimlikler, kimliklerin sahteciliğe karşı korunmasını sağlarlar. Böylelikle kullanıcıların kimlik bilgilerinin güvenliğinin artırılması ve kötü niyetli saldırılara karşı korunması sağlanır. Dijital kimlikler sayesinde kullanıcılar, paylaşmak istedikleri bilgileri seçebilir ve kimlik bilgilerinin geri kalan kısmını gizli tutabilirler. Kullanıcıların dijital kimlikler üzerindeki kontrolü, kullanıcıların gizliliklerini ve mahremiyetlerini korumalarına ve kişisel verilerinin kontrolünü ellerinde tutmalarına olanak tanır. Dijital kimlikler, doğrulayıcılar tarafından hızlı ve güvenli bir şekilde kontrol edilebilerek kimlik doğrulama süreçlerinin daha şeffaf ve güvenilir hale gelmesine olanak tanır. Dijital kimlikler, farklı platformlarda ve hizmetlerde

kullanılabilir. Bu, kullanıcıların kimliklerini ve niteliklerini kolayca taşıyabilmesine ve erişebilmesine olanak tanır. Ayrıca fiziksel belgelerin taşınması ve saklanması yerine, dijital ortamda güvenli ve kolay bir şekilde erişilebilir hale getirilir.

2.2. Doğrulanabilir Kimlikler

Doğrulanabilir kimlikler, dijital kimliklerin dijital ortamda doğrulanması için World Wide Web Consortium (W3C) tarafından standartlaştırılmış olan güvenlik ve doğrulama yöntemlerini içerir. W3C organizasyonunun biri doğrulanabilir kimliklerin veri modelini açıklayan (Sporny, Longley ve Chadwick, 2019), diğeri de doğrulanabilir kimliklerin kullanım durumlarını örnekleyen (Otto vd., 2019) iki yayını bulunmaktadır. W3C veri modeli ile ilgili yayında doğrulanabilir kimlik ekosistemde kimlik sağlayıcı, kimlik sahibi ve kimlik talep eden rollerini tanımlamıştır. Kimlik sağlayıcı, doğrulanabilir kimlik oluşturarak kimlik sahibine gönderen rolü tanımlamaktadır. Kimlik sahibi, kimlik sağlayıcıdan aldığı doğrulanabilir kimlikleri dijital cüzdanında saklar. Kimlik talep eden ise kimlik sahibinin bir kimliğini veya kimliğindeki bir bilgiyi ispatlamasını isteyebilir. Bu durumda kimlik sahibi, doğrulanabilir kimliğindeki bilgilerin tamamını veya bir kısmını içeren bir kimlik ispatı oluşturarak kimlik talep edene gönderir. Tüm bu akışlarda doğrulama için kullanılan kimlik tanımlayıcıları ile imza doğrulama açık anahtarları doğrulanabilir veri kayıt defterinde tutulur.

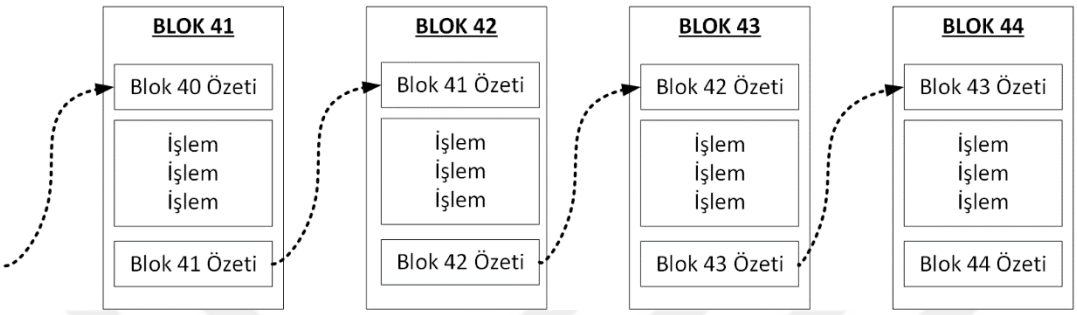
Doğrulanabilir kimlikler kullanılarak yapılan kimlik oluşması ve kimlik ispatı süreçleri ile şu bilgiler garanti edilmiş olur:

- Bir kimliğin hangi kimlik sağlayıcı tarafından verildiği
- Kimliğin gerçekten kimlik ispatını sunan varlığa verildiği
- Kimlik bilgilerinin değiştirilmediği
- Kimlik sağlayıcının kimliğin geçerliliğini sonlandırmadığı

2.3. Blok Zinciri

Blok zinciri teknolojisi, adından da anlaşılacağı üzere, Şekil 2.1.'de gösterildiği gibi birbiriyle kriptografik olarak bağlantılı "blok" adı verilen veri yapılarının bir "zincir" şeklinde sıralanmasıyla oluşur. Her blok, genellikle işlem bilgilerini, bir zaman damgasını

ve önceki bloğun kriptografik özeti olan bir “hash” değerini içerir. Bu yapı, blok zincirinin değiştirilmesi ve geçmiş işlemlerin manipüle edilmesi zor bir hale getirir. Bu teknoloji, 2008 yılında Satoshi Nakamoto tarafından geliştirilen ve kripto para birimi Bitcoin'in temelini oluşturan bir dizi kavram ve protokol üzerine kuruludur (Nakamoto, 2009).



Şekil 2.1. Blok zinciri

Blok zinciri teknolojisi, farklı kullanım senaryoları ve gereksinimler göz önünde bulundurulduğunda açık (izin gerektirmeyen) ve özel (izin gerektiren) olmak üzere iki ana türe ayrılır. Açık blok zincirleri, herkese açık ve katılımcıların işlemleri gerçekleştirebilmesine, blokları doğrulayabilmesine ve yeni bloklar ekleyebilmesine olanak veren sistemlerdir. Bu tür blok zincirlerin en önemli avantajı, merkezi olmayan ve güvenilir bir yapı sunmasıdır. Bununla birlikte, açık blok zincirleri genellikle ölçeklenebilirlik ve gizlilik konusunda sorunlar yaşayabilir. Bitcoin ve Ethereum gibi kripto para birimleri, açık blok zincirlerine örnek olarak gösterilebilir. Bu sistemlerde, herhangi bir merkezi otoriteye bağlı olmaksızın işlemler gerçekleştirilebilir ve tüm katılımcılar tarafından denetlenebilir. Özel blok zincirler ise, belirli bir organizasyon veya grup tarafından yönetilen ve sadece yetkili kullanıcıların erişebildiği sistemlerdir. Bu tür blok zincirlerin avantajları arasında ölçeklenebilirlik, gizlilik ve kontrol edilebilirlik bulunmaktadır. Özel blok zincirler, daha hızlı işlem süreleri ve daha düşük işlem maliyetleri sunarak, özel kullanım durumları için uygundur. Bununla birlikte, merkeziyet düzeyi arttığı için güven ve denetlenebilirlik konularında açık blok zincirlerine göre daha düşük seviyelerde bulunabilir.

Blok zinciri teknolojisi, katılımcıların ağ üzerindeki işlemleri ve yeni eklenen blokları doğrulamasını sağlayan konsensus mekanizmaları kullanır. Konsensus mekanizmalarının temel amacı, ağdaki düğümlerin (katılımcıların) uyumlu bir şekilde çalışmasını sağlamak ve doğru veri setinin korunarak tüm düğümlerde güncellenmesini sağlamaktır. Blok zinciri sistemlerinde kullanılan birçok konsensus mekanizması bulunmaktadır. İş Kanıtı (Proof of

Work – PoW), en bilinen ve ilk konsensus mekanizmasıdır. Bitcoin ve Ethereum gibi açık blok zincirlerinde kullanılır. PoW, düğümlerin karmaşık matematiksel problemleri çözmelerini gerektirir. Bu problemleri çözen düğüm, yeni bir blok ekler ve ödül alır. PoW mekanizması, ağa saldırı yapmayı zor bir hale getirerek güvenliği sağlar. Bununla birlikte, PoW enerji tüketimi yüksek olduğu için çevre ve maliyet açısından sürdürülebilir olmayabilir. Pay İspatı (Proof of Stake – PoS) ise enerji tüketimini azaltmayı amaçlayan alternatif bir konsensus mekanizmasıdır. PoS'ta düğümler blok eklemek için madencilik ile uğraşmak yerine, kripto paralarını pay olarak kilitleyerek katılır. Düğümlerin blok üretme ve doğrulama olasılığı, pay miktarlarına ve belirli kural setlerine bağlıdır. PoS, enerji verimliliği sağlasa da zengin düğümlerin ağı domine etme riski taşıyabilir.

Blok zinciri teknolojisinin birçok soruna çözüm potansiyeli taşımasına karşın, birçok iş kolunda geniş çapta bir kullanım alanına ulaşamamıştır. Bunun teknik sebeplerinin yanı sıra teknolojinin nasıl çalıştığı ve potansiyel kullanım durumları hakkında yeterli farkındalık ve bilgi sahibi olunmaması da yaygın kullanılmamasında bir etkendir. Bu nedenle bu teknolojinin kullanımı ile ilgili çeşitli araştırmalar yapılmıştır (Lodder ve Khovratovich, t.y.). Bu teknolojiye olan ilginin ve geliştirilen kullanım durumlarının zamanla artması ile gelecekte birçok alanda bu teknolojinin geleceği şekillendirecek bir potansiyele sahip olduğu görülmektedir.

2.4. Akıllı Sözleşmeler

Akıllı sözleşmeler, önceden tanımlanmış olan koşullar sağlandığında tetiklenen blok zinciri ağlarında otomatik olarak çalışan kod parçalarıdır. Blok zinciri ağında dağıtık olarak yer alırlar ve ağdaki düğümlere kurulurlar. Bu nedenle, ağın katılımcıları bu akıllı sözleşmelerin nasıl çalıştığını bilirler ve bu konuda ortak bir anlayışa sahiptirler. Bu, tarafların sözleşme koşullarını denetlemesine ve güvenilirliğini sağlamasına olanak tanır. Tıpkı gerçek dünya sözleşmelerinde olduğu gibi, akıllı sözleşmeler de tarafların aralarında anlaştıkları kodu çalıştırarak gerçekleşmesi gereken işlemin yerine getirilmesini sağlar. Akıllı sözleşmeler, blok zinciri üzerinde saklandığı için değiştirilemez ve şeffaftır.

2.5. Hyperledger

Hyperledger, kurumsal seviyede blok zinciri uygulamaları geliştirmeye yönelik olarak açık kaynak alt yapılar, araçlar ve kütüphaneler sunan bir ürün ailesidir. Hyperledger çatısı altında belli amaçlara yönelik olarak özelleştirilmiş birçok blok zinciri alt yapısı bulunmaktadır. Linux Vakfı tarafından desteklenen ve 2015 yılında başlatılan Hyperledger projesinin temel hedefi, endüstriler arası iş birliğini destekleyerek, blok zinciri teknolojilerini kullanarak iş süreçlerinin ve uygulamalarının güvenliğini ve etkinliğini artırmaktır.

Hyperledger Fabric, Hyperledger projesi kapsamında geliştirilen açık kaynaklı bir blok zinciri platformudur. IBM ve Digital Asset gibi büyük teknoloji şirketlerinin katkılarıyla geliştirilen Hyperledger Fabric, modüler ve ölçeklenebilir bir yapı sunarak, özellikle işletmeler ve kurumsal kullanıcılar için özelleştirilebilir blok zinciri çözümleri sağlamaktadır. Ağ katılımcılarının kimlik bilgilerini ve rollerini belirleyen ve doğrulayan bir sistem sunarak, sadece yetkilendirilmiş kullanıcıların ağa erişimine izin verir. Açık bir blok zinciri yapısı olmadığından sınırlı katılımcılar arasında kısmi güven esasına dayalı mutabakat mekanizmaları ile açık blok zinciri platformlarına göre çok daha verimli ve performanslı bir alt yapı sağlar. Platform tarafından Kafka ve Raft gibi mutabakat mekanizmaları desteklenmektedir.

Hyperledger Fabric, iş süreçlerini ve iş mantığını otomatikleştirebilmek için akıllı sözleşmeleri desteklemektedir. Akıllı sözleşmelerin Hyperledger Fabric platformundaki gerçekleştirimine zincir kodu (chaincode) adı verilmektedir. Akıllı sözleşmeler bu platformda Go ve Javascript/Typescript programlama dilleriyle yazılabilmektedir.

Hyperledger Indy, Hyperledger projesi kapsamında geliştirilen ve doğrulanabilir kimlik ve dijital kimlik konusunda özelleştirilmiş, açık kaynaklı bir blok zinciri platformudur. Hyperledger Indy'nin ana odak noktası, dijital kimliklerin yönetimi ve güvenilir, gizli ve verimli bir şekilde paylaşılmasıdır. Bu platform, kişilerin ve kurumların dijital kimliklerini oluşturmak, kontrol etmek ve doğrulamak için kullanılabilir. Hyperledger Indy ile birlikte Hyperledger ailesinden Aries ve Ursa kütüphaneleri de dijital kimlik uygulamaları geliştirmek için sunulan yardımcı araçlardır. Hyperledger Aries, daha çok dijital kimliklerle

ilgili uygulama geliştirme konusunda kütüphaneler sunarken Hyperledger Ursa ise uygulamaların güvenliğini sağlamaya yönelik olarak kriptografik kütüphaneler sunmaktadır.

2.6. Sıfır Bilgi İspatı

Sıfır bilgi ispatı (Zero Knowledge Proof – ZKP) ilk olarak Goldwasser, Micali ve Rackoff (1985) tarafından ortaya atılmıştır. Sıfır bilgi ispatı, bir tarafın (istemci) diğer tarafa (doğrulayıcı) bir önermenin doğru olduğunu kanıtlarken, önermeyle ilgili herhangi bir bilgi açıklamadan gerçekleşen bir kriptografik protokoldür. Başka bir deyişle sıfır bilgi ispatı, birinin belirli bir bilgiye sahip olduğunu kanıtlamasına izin verirken, bu bilginin kendisi hakkında hiçbir şey ortaya çıkarmaz. Sıfır bilgi ispatları, gizlilik ve güvenlik açısından önemli avantajlar sunar ve bu nedenle kriptografi ve güvenli iletişim alanlarında büyük bir değer taşır. Sıfır bilgi ispatının özellikleri Groth (2010) tarafından şu şekilde açıklanmıştır:

- Tamamlık: Eğer önerme doğruysa, dürüst bir istemci doğrulayıcıyı ikna edebilir.
- Sağlamlık: Eğer önerme yanlışsa, hiçbir kötücül istemci doğrulayıcıyı ikna edemez.
- Sıfır bilgi: Eğer önerme doğruysa, doğrulayıcı, istemcinin bildiği bilgi dışında hiçbir şey öğrenmez.

Hyperledger Indy, sıfır bilgi ispatı özelliğine sahiptir ve doğrulanabilir kimlik bilgileri sahiplerinin, kimlik özniteliklerileriyle ilgili eşitlik ve eşitsizlik beyanlarını kanıtlamak için sıfır bilgi ispatları oluşturmasına olanak tanır. Örneğin, işveren bilgisi vermeden istihdam edildiğini veya doğum tarihi belirtilmeden 18 yaşından büyük olduğunu kanıtlamak sıfır bilgi ispatıyla mümkündür.

3. LİTERATÜR ARAŞTIRMASI

Bu bölümde tez çalışması kapsamında ele alınan e-ticaret dijital kimlik güven çerçevesi ve e-ticaret itibar sistemleri alanlarında diğer araştırmacılar tarafından gerçekleştirilen mevcut çalışmalar ele alınmaktadır.

3.1. Dijital Kimlik Güven Çerçevesi

Dijital kimlik güven çerçevesi ile ilgili mevcut çalışmalara bakıldığında, bu çalışmaların çoğunluğunun ülkelerin ulusal dijital kimlik sistemlerini oluşturma çabalarına yönelik olduğu görülmüştür. Bu çalışmaların bir kısmı akademik çalışmalar olmakla birlikte bir kısmı da ulusal ve uluslararası kuruluşların yaptığı araştırmalardır. En büyük uluslararası kuruluşlardan biri olan Birleşmiş Milletler (BM), Güney Doğu Asya'da yer alan ülkelerde ulusal düzeyde uygulanan dijital kimlik yaklaşımlarını incelemiş ve elde ettiği bulgulara dayanarak bu ülkelerin dijital kimlik kullanımına geçişleri için bulguların ve önerilerin yer aldığı bir rapor yayınlamıştır (BM, 2020). Başka bir dijital kimlik çalışması ise Dünya Bankası (DB) tarafından yapılan ve Group of 20 (G20) ülkelerini kapsayan bir çalışmadır. Bu çalışmada DB, dijital kimliğin finansal kuruluşların faaliyetleri bakımından kullanım potansiyellerini ve bu kuruluşlardaki uygulamalarını incelemiş ve yetkililere bu konuda izlenebilecek politikalara yönelik tavsiyelerde bulunmuşlardır. Tüm dünyadaki insanların dijital medeni haklarını savunmak amacıyla 2009 yılında kurulan AccessNow adlı kuruluş ise insan hakları açısından dijital kimlik uygulamalarını değerlendirmiş ve bu bağlamda yönetim, denetim, kontrol, bilgi güvenliği, gizlilik ve siber güvenlik konularında yetkililere politika önerileri sunmuştur (AccessNow, 2018). Dünya Ekonomik Forumu (DEF), tedarik zinciri uygulamalarında dijital kimliğin kullanımına yönelik bir çalışma gerçekleştirmiş ve dijital kimlik güven çerçevesi temel bileşenlerinin yer aldığı bir kılavuz hazırlamıştır (DEF, 2019). ITU'nun 2018 yılında hazırladığı Dijital Kimlik Yol Haritası Kılavuzu, yetkililere ülkelerin dijital kimlik politikalarını belirlemede yol gösterici niteliğinde kapsamlı bir kılavuzdur (ITU, 2018). Yine DB'nin bir inisiyatifi olan ID4D (Identification for Development) de benzer bir amaca yönelik olarak dijital kimlik uygulama kılavuzu hazırlamıştır (DB, 2019). Dijital kimlik kullanımının yaygınlaştırılmasını ve çok daha fazla insana ulaşmasını hedefleyen ID2020 birliği on maddelik bir bildiri yayınlayarak bu konudaki yaklaşımlarını ifade etmişlerdir (ID2020, 2018). Ayrıca ID2020 birliği, dijital

kimlik alanında çözümler üreten teknoloji şirketlerinin ID2020 kurallarına uygunluğunun sertifikasyonu için teknik gereksinimler paylaşmıştır (ID2020, 2019).

Uluslararası kuruluşlar dışında bazı ülkelerdeki ulusal kuruluşlar da ulusal düzeyde dijital kimliğin kullanımına yönelik olarak çalışmalar yapmışlar ve kılavuzlar hazırlamışlardır. Amerika Birleşik Devletleri'nde (ABD) 2018 yılında kurulmuş olan Daha İyi Kimlik Koalisyonunun (Better Identity Coalition) hazırladığı yol haritası, ABD'de güvenli bir dijital kimlik alt yapısı kurulmasına yönelik bir kılavuzdur (The Better Identity Coalition, 2019). Ulusal düzeyde dijital kimlik güven çerçevesi oluşturan ülkelerden biri olan Yeni Zelanda, oluşturdukları güven çerçevesinin prensiplerini ve unsurlarını yayınlamışlardır (Yeni Zelanda Hükümeti, 2020). Birleşik Krallık ise ulusal düzeyde dijital kimlik uygulamaları için İyi Uygulama Rehberi (Good Practice Guide – GPG) adını verdikleri birçok kılavuz yayınlamıştır. Bu kılavuzlar, dijital kimlik uygulanmalarını farklı açılardan ele alan birçok başlığı kapsamaktadırlar. Bunlardan biri, kişilerin kimliklerini kanıtlaması ve kimliklerin doğrulanması ile ilgili adımları ve açıklamaları içeren "GPG 45: How to prove and verify someone's identity" adlı kılavuzdur (National Technical Authority for Information Assurance [CESG], 2014). Bir diğeri çevrim içi sunulan hizmetlerin güvenliği için kimlik doğrulamanın kullanılması ile ilgili olan "GPG 44: Using authenticators to protect an online service" isimli kılavuzdur (CESG, 2013). Yine çevrim içi hizmetlerin güvenli bir şekilde sunulabilmesine yönelik "GPG 43: Requirements for Secure Delivery of Online Public Services" isimli bir kılavuz bulunmaktadır (CESG, 2012). İyi uygulama rehberlerinden bir diğeri de dijital kimliklerin kişiler dışında kuruluşlara da uygulanması ile ilgili olan "GPG 46: Organisation Identity" isimli kılavuzdur (CESG, 2013). Bu kılavuz, dijital kimliğin kişiler dışında başka varlıklara, özellikle de firma ve kuruluşlara da uygulanabileceğini gösteren literatürde az rastlanan çalışmalardan biridir. Dijital kimliğin kuruluşlara uygulanmasına yönelik olarak yapılan bir diğer çalışma da Kanada'nın gerçekleştirdiği dijital kimlik güven çerçevesidir. Kanada'nın dijital kimlik güven çerçevesi, bu alanda yapılan en ayrıntılı çalışmalardan olup güven çerçevesinin bileşenlerini ve adımlarını detaylı bir şekilde ortaya koymaktadır. Bu ve benzeri dijital kimlik çalışmalarına yönelik özel olarak kurulan The Digital Identification and Authentication Council of Canada (DIACC), Kanada'ya özgü bir dijital kimlik güven çerçevesi oluşturmuştur (DIACC, 2020). DIACC'ın ortaya koyduğu ve Pan-Canadian Trust Framework (PCTF) olarak adlandırdığı dijital kimlik güven çerçevesi hem kişilere hem de kuruluşlara güvenli bir şekilde dijital kimlik

verilebilmesi için izlenmesi gereken aşamaları, kimlik kullanımı ve yaşam döngüsü bağlamında neler yapılması gerektiğini ayrıntılı bir biçimde ele alır.

Dijital kimlik güven çerçevesi alanında çalışan bazı kuruluşlar ise belli bir ülkeye özel olmayan daha üst seviyede çalışmalar gerçekleştirmişlerdir. Bu kuruluşlardan biri olan Open Identity Exchange topluluğu, 2010 yılında ilk defa yayınladıkları ve "Open Identity Trust Framework" adını verdikleri Açık Kimlik Güven Çerçevesi modelini geliştirmişlerdir (Maler, Nadalin, Reed, Rundle ve Thibeau, 2010). Bu geniş çaplı modelde, güven çerçevesinde yer alan rollerin sadece kimlik sağlayıcı, kullanıcı ve hizmet sağlayıcı üçlüsünden oluşmadığı, bunlar dışında dijital kimlikle ilgili politikaların belirlenmesi konusunda yetkili merciler, güven çerçevesi kapsamındaki hizmet sağlayıcıları, akreditasyon ve uyum denetimi için değerlendirme ve denetleme organizasyonları ve ortaya çıkabilecek ihtilaflı konular için ara bulucular gibi çok farklı rollerin de güven çerçevesinin unsurları olduğunu ortaya koymuşlardır. Topluluk 2010 yılındaki bu yayınından sonra çok daha detaylı kılavuzlar ve raporlar hazırlamışlardır. Topluluk, dijital kimlik güven çerçevesi unsurlarının ele alınmasında nasıl bir yaklaşım izlenmesi gerektiği ile ilgili 2020 yılında ayrıntılı bir kılavuz hazırlamıştır (Mothershaw, 2020). Bu alanda üst seviyede çalışma yapan kuruluşlardan bir diğeri de Amerika Birleşik Devletleri Ulusal Standartlar ve Teknoloji Enstitüsü'dür (NIST). NIST, dijital kimlik güven çerçevesi konusunu federe kimlik sistemleri açısından ele alan birçok yayın yapmıştır (Grassi, Garcia ve Fenton, 2017; Grassi, Fenton, Newton, Perlner ve Regenscheid, 2017; Grassi, Richer, Squire, Fenton, ve Nadeau, 2017; Temoshok ve Abruzzi, 2018).

Dijital kimliklere yönelik olarak yapılmış olan akademik çalışmalarda güven çerçevesi özelinde yapılan çalışmaya az rastlanmıştır. Bu alanda Lim (2020) tarafından yapılan çalışma, kullanıcı egemen kimliklere yönelik olarak güven çerçevesi oluşturulmasına yöneliktir. Lim, güven çerçevesinin oluşturulması için ön şart olarak gördüğü güven çerçevesinin yönetişim yönü ve yasal yönü konusunda ortak bir anlayışa varılması gerektiğini ifade etmiştir. Lim buna yönelik olarak kullanılmak üzere Trust Over IP (TOIP) modelini önermiştir. Literatürde güven çerçevesi özelinde olmayan, dijital kimlik alanında blok zincirinin kullanımını ele alan çalışmalara daha çok rastlanmıştır. Bu alanda Goodell ve Aste (2019) yaptıkları çalışmada dağıtık kayıt defteri yapısını kullanan ademi merkeziyetçi bir dijital kimlik mimarisi önermiştir. Bu öneri ile kullanıcı bilgilerinin gizliliğinin korunmasına yönelik gerekli kriterleri tanımlayarak bu kriterlere uyan dağıtık

kayıt defteri teknolojisine dayalı bir öneri sunmuşlardır. Jamal, Helmi, Syahirah ve Fatima (2019) ise dijital kimlikleri tutmak ve bunlar üzerinden kimlik doğrulama yapmak için blok zincirinin kullanılabileceği bir çözüm önermişlerdir. Fakat bu çalışmada kullanıcıların kimlik bilgilerinin gizliliğinin korunmasına ilişkin herhangi bir çözüm önerisi getirilmemiştir. Dijital kimliklerin blok zincirinde saklandığı kimlik yönetim modelinin kullanıcı egemen kimlik yönetimi olduğu, dolayısıyla kimlik bilgilerinin mahremiyetini dikkate alan bir diğer dijital kimlik çalışması da Liao, Guan, Cheng ve Yuan (2022) tarafından yapılan çalışmadır. Liao ve diğerleri Ethereum blok zincirinde çalışan bir çözüm sunarak blok zincirine dayanan dijital kimlikleri açık bankacılık bağlamındaki senaryolarda kullanmıştır. Dissanayake ve diğerleri (2021) "Trust Pass" diye adlandırdıkları blok zincirine dayanan dijital kimlik çözümü ile kimlik kanıtı ve dijital kimlik ispatı aşamalarını gerçekleştirmişlerdir. Yapay sinir ağları üzerine kurdukları bu sistem ile başarımı yüksek bir belge ve biyometrik veri doğrulama sistemi ortaya koymuşlardır. "Trust Pass" sisteminde kimlik bilgilerinin gizliliğinin korunması ve veri güvenliğinin sağlanması amacıyla bu veriler blok zincirinde saklanmıştır. Argento ve diğerleri (2020) ise katılımcıların blok zinciri kullanarak gerçekleştirdikleri işlemlere, Avrupa Birliği tarafından yayınlanan “electronic identification and trust services for electronic transactions in the internal market” (eIDAS) yönetmeliğine uygun olan ulusal dijital kimlik sistemlerinin dahil edildiği bir model önermişlerdir. Bu model ile blok zinciri kullanılarak yapılan işlemlerde katılımcıların ulusal kimlik sistemi üzerindeki kimliklerine eşlenmesi, yapılan işlemlerin reddedilememesi, işlemlere ilişkin denetim kayıtlarının saklanması ve takip edilebilmesi sağlamıştır. Gada, Dhuri, Jain, Bansod ve Toradmalle (2021) ise blok zincirine dayalı dijital kimlik yönetimi modelini kullanarak Ethereum blok zincirinde çalışan bir kitle fonlama sistemi geliştirmiştir.

Blok zinciri üzerinde çalışan dijital kimlik kullanılarak geliştirilmiş çözüm önerilerinin dışında, literatürde dijital kimliklerin kullanımıyla, yaşam döngüsüyle ve kimlik ispatlarıyla ilgili yapılmış olan çalışmalara da rastlanmaktadır. Pöhn ve Hommel (2020), kimlik yönetim sistemlerinin karşılaması gereken kriterleri tanımlayarak, hali hazırdaki kimlik sistemlerinin eksik noktalarını ve yeni yaklaşımların gerekliliğini belirtmişlerdir. Rasouli, Valmohammadi, Azad ve Esfeden (2021) tarafından yapılan bir çalışmada stratejik planlamanın dijital kimlik yönetimi bağlamında en etkili ana unsur olduğunu tespit etmişlerdir. Bu çalışmaya on alan uzmanı katılmış ve belirlenen altı ana faktör ile otuz bir alt faktörün dijital kimlik yönetiminde ne kadar önemli olduğu incelenmiştir. Akram ve Sen

(2022) tarafından gerçekleştirilen olay analizi çalışmalarında bankacılık, finans ve sigortacılık alanlarındaki olaylar için sıfır bilgi ispatını da içeren blok zincirine dayalı dijital kimlik çözümleri incelenmiştir. Lim ve diğerleri (2018) ise blok zincirine dayalı dijital kimlik yaşam döngüsü ve ispatına yönelik 2014 – 2018 arasında ortaya koyulan çözüm önerilerini incelemişlerdir. Bu incelemenin sonunda yayınladıkları raporda incelenen çözüm önerilerinin eksik yönlerini ve iyileştirme noktalarını belirtmişlerdir. Liu ve diğerleri (2020) yaptıkları çalışmada dijital kimlik sistemlerini kimlik sahiplerinin kimlikleri üzerinde ne kadar kontrole sahip oldukları yönünden değerlendirmişlerdir. Bu araştırma ile blok zincirine dayalı veya benzer şekilde dağıtık kayıt defteri kullanan dijital kimlik sistemlerinin bu amaca yönelik olarak daha uygun olabileceği yönündeki değerlendirmelerini belirtmişlerdir. Gruner ve diğerleri (2018) blok zincirine dayalı dijital kimlik çözümlerinin ne derece güvenilir olduğunu sayısal olarak belirlemeye yönelik bir model önerisi sunmuşlardır. Aynı çalışmada, belirlenen sayısal değerlere karşılık gelen kalitatif güvenilirlik düzeylerini de tanımlamışlardır (Gruner vd., 2018).

3.2. İtibar Sistemi

Bu bölümde, itibar sistemleri alanında diğer araştırmacılar tarafından gerçekleştirilen mevcut çalışmalar aşağıdaki alt başlıklarda gruplanarak verilmiştir.

- Açık blok zincirler üzerine geliştirilen e-ticaret itibar sistemleri,
- Açık blok zincirler üzerine geliştirilen e-ticaret dışındaki diğer itibar sistemleri,
- Özel blok zincirler üzerine geliştirilen e-ticaret itibar sistemleri
- İtibar sistemlerine yönelik yapılmış olan literatür taraması çalışmaları
- Blok zinciri teknolojisine alternatif olarak merkezi defter veri tabanlarına yönelik çalışmalar

3.2.1. Açık blok zincirler üzerine geliştirilen e-ticaret itibar sistemleri

Literatürde Bitcoin ve Ethereum gibi açık blok zincirleri ve kripto para birimleri üzerine inşa edilmiş merkezi olmayan blok zinciri tabanlı itibar sistemlerine yönelik birçok araştırma bulunmaktadır. Bu sistemlerden bazıları, geri bildirim gönderen kullanıcıların mahremiyetini korumaya odaklanmışken diğerleri ise mahremiyet konusunu göz ardı etmişlerdir.

Sun, Liu ve Guo (2019) harcanan jetonlarla orantılı bir ağırlığa sahip olacak şekilde geri bildirim puanları göndermek için "itibar jetonları" harcayarak bazı saldırı türlerini önlemeyi amaçlamışlardır. Düğümlerin, blok zinciri ağında blok oluşturdukları sürece jeton kazanmaları beklenir. Araştırmacılar bu modelin geri bildirimi yapan kişinin mahremiyetini koruyacağını düşünseler de modelde alıcıların daha fazla jeton kazanarak geri bildirim göndermeleri için herhangi bir teşvik mekanizması bulunmamaktadır. Schaub, Bazin, Hasan ve Brunie (2016) bazı saldırı türlerini önlemek için gizliliği koruyan kapsamlı bir itibar sistemi önermişlerdir. Bu modelin ana bileşeni, alıcının geri bildirim göndermesine olanak sağlamak için satıcı tarafından alıcıya verilen körleştirilmiş jetondur. Satıcının jeton üretebilmesi için sistemin alt yapısında bulunan blok zincirinden kripto para kazanması ve harcaması gerekir. Owiyo, Wnag, Asamoah, Kamenyi ve Obiri (2018), Schaub ve diğerleri tarafından önerilen modele çok benzer bir model önermişlerdir. Bununla birlikte, her iki modelde de satıcıların nasıl jeton kazanacakları ve alıcılara jeton sağlamak için nasıl yeterli jetona sahip olacakları açık değildir. Carboni, Bitcoin ödemelerine dayanan Bitcoin tabanlı bir itibar sistemi önermiştir (Carboni, 2015). Bu modelde Bitcoin adresleri, geri bildirim veren kullanıcıların gizliliğini korumak için kullanılmıştır. Soska, Kwon, Christin ve Devadas (2016) ise Beaver adını verdikleri merkezi olmayan bir pazar yeri ile entegre bir itibar sistemi önermişlerdir. Önerilen çözüm, itibar sistemi saldırılarına karşı korumada umut verici görünse de tamamen merkezi olmayan pazar yeri mimarisi ve kripto para birimi tabanlı ödemeler üzerine kurulu olması, mevcut e-ticaret uygulamaları ile birlikte çalışabilirlik bakımından kısıt getirmektedir.

Yukarıda bahsedilen çalışmalar kullanıcı mahremiyetini dikkate alan çalışmalardır. Bu çalışmaların yanı sıra kullanıcı mahremiyetini dikkate almayan çalışmalar da bulunmaktadır. Bu çalışmaların çoğunluğu Ethereum blok zinciri alt yapısı üzerine kurulmuştur. Tamang (2018), açık bir blok zinciri ağı olan Ethereum'a dayalı modelinde bazı saldırıları önlemek için "Toplam Onay Etkisi" puanı hesaplamıştır. Bu puanın hesaplanması, onaylayanların ve onaylananların hem gelen hem de giden bağlantılarına dayanır. Bu da bir e-ticaret sistemi için beklenmedik itibar puanlarının ortaya çıkmasıyla sonuçlanabilir. Dhakal ve Cui (2019) ise DTrust olarak adlandırdıkları başka bir Ethereum tabanlı itibar sistemi önermişlerdir. DTrust'un kısıtları, sadece Ethereum üzerinden gerçekleştirilen ödemelere bağımlı olması ve geri bildirim veren kullanıcıların mahremiyetini korumayı dikkate almamasıdır. Zulfiqar ve diğerleri (2021) EthReview olarak adlandırdıkları ve DTrust ile benzer kısıtlara sahip Ethereum tabanlı bir itibar sistemi önermişlerdir. Wang, Zhang ve Kim (2018) de

ReviewChain adını verdikleri Ethereum tabanlı bir itibar sistemi önermişlerdir. ReviewChain, e-ticaret uygulamalarından ziyade blok zinciri üzerine kurulu tedarik zinciri sistemleri için tasarlanmıştır. Almasoud (2020) da yaptığı tez çalışmasında e-ticaret pazar yerleri için Ethereum tabanlı bir itibar sistemi önermiştir. Bu itibar sisteminde geri bildirim aşaması e-ticaret oturumunun ayrılmaz bir parçası olarak kurgulanmıştır. Bu nedenle mevcut e-ticaret sistemleri ile birlikte çalışabilirlik konusunda kısıtları bulunmaktadır.

Literatürde kullanıcı mahremiyetini dikkate almayan çalışmalardan Ethereum blok zinciri dışındaki başka açık blok zincirlerine bağlı olarak geliştirilmiş itibar sistemi önerileri de bulunmaktadır. Ahn, Park, Shin ve Paek (2019) satın alma işlemlerini ve geri bildirimleri blok zincirinde saklayan ve Bitcoin kripto para birimi tabanlı ödeme sistemleri üzerine kurulu bir itibar sistemi önermişlerdir. Bu sistemin kısıtı, kripto para birimi tabanlı ödeme sistemine bağımlılığıdır. Buechler ve Hockenbrocht (2015) ise Bitcoin ağı ve Ethereum akıllı sözleşmeleri üzerine kurulu, kendilerine özgü itibar puanını hesaplama algoritmasına sahip merkezi olmayan bir itibar sistemi önermişlerdir. Ramachandiran'ın (2018) önerdiği model, biri geri bildirim kayıtlarını diğeri ise alıcı ve satıcı bilgilerini tutmak üzere iki blok zinciri içermektedir. İkinci blok zinciri, alıcı ve satıcı kayıtlarıyla bağlantılı olan satın alma kayıtlarını da tutmaktadır. Mevcut bir e-ticaret sisteminde hali hazırda tutulan bilgilerin fazladan bu modelde önerilen blok zincirinde de tutulması, bu bilgilerin senkron tutulması için ek bir maliyet ve yük getirmektedir. Bunun yanında, alıcı bilgileri de blok zincirinde saklandığından alıcı mahremiyeti korunmamaktadır.

3.2.2. Özel blok zincirler üzerine geliştirilen e-ticaret itibar sistemleri

Kugblenu ve Vuorimaa (2020) tarafından önerilen itibar sistemi bir özel blok zinciri ile geliştirilmiş çok az sayıdaki itibar sisteminden biridir. Bu itibar sistemi, yalnızca ürün kimliği, satıcı kimliği ve sipariş kimliği bilgilerinin birleştirilmesiyle oluşturulan bir metin ile ödeme adımında geri bildirim jetonu oluşturarak gizliliği korumaya çalışır. Fakat bu geri bildirim jetonunda dijital imza ve kriptografik doğrulama gibi mekanizmalar bulunmamaktadır. Özel blok zinciri alt yapısı kullanan diğer bir itibar sistemi de RepChain'dir (Li vd., 2021). RepChain kullanıcı mahremiyetini korumak için kör imza yöntemini kullanır.

3.2.3. Açık blok zincirler üzerine geliştirilen diğer itibar sistemleri

Mevcut çalışmalarda e-ticaret alanı dışında başka sektörlerde kullanılmak üzere geliştirilmiş olan merkezi olmayan itibar sistemleri de bulunmaktadır. Mendes ve diğerleri mobil uygulamalara ilişkin geri bildirimleri mobil uygulama mağazalarında saklamak için blok zinciri tabanlı bir itibar sistemi oluşturmuşlardır (Mendes, Chen, Silva, Serrao ve Casal, 2021). Benzer görünseler de mobil uygulama ile e-ticaret geri bildirim sistemleri birçok yönden farklılıklar göstermektedirler. Merkezi olmayan itibar sisteminin başka bir örneği ise, Omori ve Kishigami (2019) tarafından açık artırmalar için kullanılmak üzere Ethereum blok zinciri üzerinde çalışan sistemdir. Park, Youn, Kim, Rhee ve Shin (2018) IoT veri pazarları için akıllı sözleşme tabanlı merkezi olmayan bir geri bildirim sistemi önermiştir. Nguyen, Bai ve Yu (2020) sosyal medya gibi kitlelerden gelen geri bildirimlerin güvenilirliğini değerlendirmek için blok zincir tabanlı bir güven modeli önermişlerdir.

Yukarıdaki üç alt başlıkta bahsedilen tüm blok zinciri tabanlı sistemler, aşağıdaki tabloda özetlenmiştir. Tez çalışmamızda önerilen itibar sistemi ile karşılaştırıldığında tabloda yer alan itibar sistemleri ile aradaki farklar şu şekilde sıralanabilir:

- Açık blok zincirlere dayalı itibar sistemleri genellikle İş İspatı gibi verimli olmayan mutabakat mekanizmalarına ihtiyaç duyarlar. Bu mutabakat mekanizmalarında işlem süresi daha uzundur ve özel blok zincirlerine göre yüksek enerji tüketimine sebep olurlar.
- Kullanıcı mahremiyetini korumayan itibar sistemleri taraflı ve art niyetli geri bildirimleri önlemekte başarılı değildirler.
- Kullanıcı mahremiyeti için kör imzaları kullanan itibar sistemleri ile karşılaştırıldığında, doğrulanabilir kimlikler sıfır bilgi ispatı ile daha yapısal ve öznitelik temelli seçimli bilgi ifşası sağlarlar.

Çizelge 3.1. Blok zinciri tabanlı itibar sistemleri

#	Başlık	Blok Zinciri Türü	Alan	Mahremiyet Koruması
1	A Model for Deriving Trust and Reputation on Blockchain-Based e-Payment System.	Açık (Bitcoin)	E-ticaret	Hayır
2	A Privacy-Preserving and Robust Reputation System Based on Blockchain.	Açık	Genel	Evet. İtibar jetonları madencilik ödülü olarak üretilir.
3	A Trustless Privacy-Preserving Reputation System.	Açık (kripto para)	E-ticaret	Evet, kör imza kullanılarak.

4	Decentralized Privacy Preserving Reputation System.	Açık (kripto para)	E-ticaret	Evet, kör imza kullanılarak.
5	Decentralized Reputation Model and Trust Framework Blockchain and Smart contracts.	Açık (Ethereum)	Genel	Hayır
6	DTrust: A Decentralized Reputation System for E-commerce Marketplaces.	Açık (Ethereum)	E-ticaret	Hayır
7	EthReview: An Ethereum-based Product Review System for Mitigating Rating Frauds.	Açık (Ethereum)	E-ticaret	Hayır
8	Feedback based Reputation on top of the Bitcoin Blockchain.	Açık (Bitcoin)	E-ticaret	Evet, Bitcoin adresleri kullanılarak.
9	Decentralized Reputation System for Transaction Networks.	Açık (Bitcoin ve Ethereum)	E-ticaret	Hayır
10	ReviewChain: Smart Contract Based Review System with MultiBlockchain Gateway.	Açık (Ethereum)	E-ticaret	Hayır
11	Smart Contracts for Blockchain-based Reputation Systems.	Açık (Ethereum)	E-ticaret	Hayır
12	Using Blockchain Technology To Improve Trust In eCommerce Reviews.	Açık	E-ticaret	Hayır
13	Beaver: A Decentralized Anonymous Marketplace with Secure Reputation.	Açık (Bitcoin)	E-ticaret	Evet, merkezi olmayan pazar yeri nedeniyle.
14	Decentralized Reputation System on a Permissioned Blockchain for E-Commerce Reviews.	Özel (Hyperledger Fabric)	E-ticaret	Evet, ürün kimliği, satıcı kimliği ve sipariş kimliğinin birleştirilmesiyle üretilen geri bildirim jetonu ile. Dijital imza ve kriptografik doğrulama içermez.
15	A Novel Reputation System for Mobile App Stores Using Blockchain.	Özel (Hyperledger Fabric)	Mobil Uygulama Mağazası	Hayır
16	Incorporating Reputation System in Blockchain-Based Distributed Auctions.	Açık (Ethereum)	Açık Artırma	Hayır
17	Smart Contract-Based Review System for an IoT Data Marketplace.	Açık (Ethereum)	IoT Veri Pazar Yeri	Hayır
18	A Blockchain-based trust model for crowd environments.	Belirtilmemiş	Kitle Fonlama	Hayır
19	Anonymous and Verifiable Reputation System for E-Commerce Platforms Based on Blockchain	Özel	E-ticaret	Evet, kör imza kullanılarak.

3.2.4. İtibar sistemleri üzerine literatür taramaları

İtibar sistemleri ile ilgili mevcut model önerisi çalışmalarının yanı sıra literatürdeki itibar sistemlerini inceleyen ve karşılaştıran çalışmalar da bulunmaktadır. Bellini, Iraqi ve Damiani (2020) blok zinciri tabanlı itibar sistemleri ile ilgili hem akademik araştırmaları hem de ticari uygulamaları incelemişlerdir. Cai ve Zhu (2016) ise blok zinciri tabanlı itibar sistemlerinin öznel ve nesnel bilgi dolandırıcılığını önleme bakımından güçlü yönlerini ve kısıtlarını incelemişlerdir. Hasan, Brunie ve Bertino (2020) itibar sistemleri üzerine geniş bir çalışma yaparak özellikle kullanıcı mahremiyetini koruyan itibar sistemlerini incelemek etmek amacıyla bir analiz sistemi oluşturmuşlardır. Oluşturdukları bu analiz sistemini kullanarak yaptıkları blok zinciri tabanlı itibar sistemlerinin karşılaştırmasına da çalışmaları kapsamında yer vermişlerdir. Andrade (2019) yaptığı tez çalışmasında blok zinciri tabanlı itibar sistemlerini tamamen teknik bir bakış açısıyla değerlendirmiştir. Almasoud, Hussain

ve Hussain (2020) blok zinciri tabanlı itibar sistemlerinde akıllı sözleşmelerin kullanımı ile ilgili sistematik bir literatür taraması gerçekleştirmişlerdir. Bu konudaki literatürde boşluk analizi yaparak, Ethereum akıllı sözleşmelerine dayanan bir itibar sistemi önermişlerdir. Battah, Iraqi ve Damiani (2021) blok zinciri tabanlı itibar sistemlerinin gerçekleştirme zorlukları ve bunlara yönelik olası çözümler üzerine çalışmışlardır. Benzer şekilde, Vandervort da Bitcoin işlemlerine dayanan itibar sistemlerinin zorlukları ve avantajları üzerine çalışma gerçekleştirmiştir (Vandervort, 2014). Basili ve Rossi (2020) özellikle araç paylaşımı hizmetlerinde itibar sistemlerinin hizmet kalitesine etkisi üzerine örnek vaka çalışmalarını incelemişlerdir.

3.2.5. Merkezi defter veri tabanları

Merkezi defter veri tabanları ve özel blok zincirler, verileri güvenli ve denetlenebilir bir şekilde yönetmek ve saklamak için tasarlanmış iki farklı teknolojidir. Merkezi defter veri tabanları, özel blok zincirlerine benzer şekilde verilerin bozulmasına karşı kanıt ve inkâr edilememe özelliklerini sağlayabilirler. Merkezi olmayan bir yapıya ve akıllı sözleşmelere ihtiyaç duyulmadığında, özel blok zincirlerine kıyasla daha yüksek verim, daha düşük gecikme süresi ve daha iyi kullanılabilirlik sağladıkları için merkezi defter veri tabanları daha iyi bir seçenek olabilir. Bu blok zinciri özelliklerine ihtiyaç olmadığı durumlarda merkezi defter veri tabanlarının kullanımına yönelik olarak yakın zamanda gerçekleştirilmiş çalışmalar bulunmaktadır (Amiri, Allard, Agrawal ve Abbadi, 2022; Fekete ve Kiss, 2021; Yang vd., 2020; Yang vd., 2022). Fakat yaptığımız literatür araştırmalarında merkezi defter veri tabanlarını kullanan bir itibar sistemine rastlanmamıştır.

Tez çalışmamızda önerdiğimiz itibar sisteminin merkezi olmayan bir yapıya sahip olması ve saklanan veri üzerinde herhangi bir otoritenin tek yetkili olmaması itibar sistemimizin anahtar özellikleridir. Saklanan verinin sahipliği, e-ticaret platformları ve satıcılar da dahil olmak üzere sistemin tüm katılımcıları tarafından paylaşılmaktadır. İtibar sistemimizde ayrıca geri bildirimlerin saklanması, itibar puanının hesaplanması ve indirim jetonlarının üretilmesi aşamalarında akıllı sözleşmeler kullanılmaktadır. Bu nedenle itibar sistemimizde merkezi defter veri tabanı teknolojisi özel blok zincire alternatif olarak değerlendirilmemiştir.

4. E-TİCARET DİJİTAL KİMLİK GÜVEN ÇERÇEVESİ

Dijital kimlik güven çerçevesi, belirli bir ekosistemdeki aktörlerin birbiriyle kurallara bağlı ilişkiler kurmasını sağlamak ve katılımcılara güvence sunmak amacıyla oluşturulan düzenlemeler topluluğudur (Mothershaw, 2020). Elektronik ticaret bağlamında tasarlanacak bir dijital kimlik güven çerçevesinin çalışmasına dair kuralların bütün ilgili taraflarca net bir şekilde anlaşılmış olması gerekmektedir ve bu tarafların belirlenen kurallara uymaları beklenir. Bu güven çerçevesi dokuz temel bileşenden oluşur:

1. İlkeler
2. Dijital Kimlik Yönetim Şeması
3. Dijital Kimlik Veri Yapısı
4. Güven Çerçevesi Rolleri
5. Dijital Kimlik Çeşitleri
6. Kimlik İspatı ve Dijital Kimlik Alma Süreci
7. Dijital Kimlik İbrazı ve Doğrulama
8. Güven İşareti
9. Güven Çerçevesi Paydaşları ve Yönetişimi

4.1. İlkeler

Dijital kimlik güven çerçevesini oluşturan tüm unsuların belirlenmesi, güven çerçevesinin hangi temel ilkeler üstüne kurulacağı ile doğrudan ilişkilidir. Dijital kimlik güven çerçevesi ile ilgili bugüne kadar yapılmış çalışmaların çoğunluğu, öncelikle güven çerçevesinin ilkelerini belirlemiştir. OITF Güven Çerçevesi (Maler vd., 2010), OIX Guide to Trust Frameworks (Mothershaw, 2020) ve PCTF (DIACC, 2020) güven çerçevelerinde tanımlanmış olan ilkeler incelenmiş ve bu tez çalışması kapsamında önerilen dijital kimlik güven çerçevesinin temel ilkeleri belirlenmiştir.

1. Güven çerçevesi, uygulanabilir uluslararası standartların bulunması durumunda o standartlara uygun olmalı ve farklı alt yapılarla oluşturulmuş standartlara dayanan başka kimlik sistemleriyle uyumluluğu dikkate almalıdır.
2. Güven çerçevesi, kimlik ispatı ve doğrulama süreçleri için uygulanacak metotların güvence düzeylerini belirleyerek bu bilgileri paydaşlarına açık bir şekilde sunmalıdır.

Bir kimlik sahibinin dijital kimliği alırken kullandığı kimlik kanıtlama yöntemlerini ve dolayısıyla kullanılan yöntemin güvence seviyesini güven çerçevesinde yer alan paydaşlar bilmelidir.

3. Firmalar kendi dijital kimlikleri ya da dijital kimliklerinde bulunan bilgileri tamamen veya kısmen paylaşma hakkına sahip olmalıdırlar. Şirketler, dijital kimlikleri üzerinde tam denetime sahip olmalıdırlar.
4. Firmalar tarafından dijital kimlikler aracılığıyla paylaşılan bilgiler, sadece belirtilen amaç için kullanılmalı, başka amaçlarla işlenmemeli ve üçüncü taraflarla paylaşılmamalıdır.
5. Firmalar, sahip oldukları dijital kimliği geniş bir yelpazede kullanabilmelidirler. Dijital kimliklerin kullanılabilirliği, e-ticaret işlemlerinin gerçekleştirildiği platformlardan bağımsız olmalıdır.
6. Güven çerçevesi içerisinde belirlenen süreçler, dijital kimlikler ve kimliklerde bulunan bilgilerin siber saldırılara ve dolandırıcılığa karşı korunmasını sağlayacak yöntemleri içermelidir.
7. Güven çerçevesinin kuralları, uygulanan aşamalar, yönetimi, denetimi ve kontrolü tüm paydaşlar tarafından bilinecek şekilde açık olmalıdır.
8. Güven çerçevesi paydaşları, güven çerçevesi kapsamında uygulanan kurallara uygun davranmalı, buna yönelik kontrolleri ve uygunluk denetimlerini kabul etmelidir. Güven çerçevesi, kurallara uygun davrandığı değerlendirilen paydaşlara verilmek üzere kurallara uygunluk belirteci olan sembol veya işaretler içermelidir.
9. Firmalar belli bir kimlik sağlayıcıdan dijital kimlik almak zorunda kalmamalı, farklı yetkili kimlik sağlayıcıların verdiği benzer bilgiler içeren dijital kimlikler güven çerçevesince desteklenmelidir.

4.2. Dijital Kimlik Yönetim Şeması

Dijital kimlik yönetimi, merkezi, federe ve dağıtık olmak üzere üç farklı yönetim şemasında gerçekleştirilebilir (DEF, 2018).

- Merkezi kimlik yönetim şemasında tüm dijital kimlik bilgileri tek bir kuruluş tarafından tutulur ve kimlik yönetimi işlemleri bu kuruluş aracılığıyla yürütülür. Bu şekilde tek bir kuruluşun kimlik işlemlerinde yetkili olduğu modele merkezi kimlik yönetim şeması denir. Bu modeldeki merkezi yetkili kuruluş Türkiye'de Nüfus ve

Vatandaşlık İşleri Genel Müdürlüğü (NVİGM) olarak karşımıza çıkmaktadır. NVİGM tüm Türkiye Cumhuriyeti vatandaşlarının kimlik bilgilerinin saklanmasından ve yönetiminden sorumludur. Ayrıca NVİGM, vatandaşların e-devlet sistemi üzerinden hizmet sağlayan diğer kuruluşların çevrim içi hizmetlerine erişebilmesi için kimlik doğrulama hizmeti de sağlar. Bu gibi merkezi kuruluşların yönettiği sistemler çok büyük bir kitlenin kimlik verilerini sakladığından, siber saldırılar için çekici hedefler hâline gelmektedir. Ayrıca kimlik verilerinin yönetimi ve paylaşılması merkezi kuruluşun kontrolünde olduğundan kimlik sahibinin kimlik bilgileri üzerinde kontrolü azdır. Bu nedenle merkezi kimlik yönetim şeması kimlik bilgilerinin gizliliğinin korunması ve kullanıcının kendi verisi üzerindeki egemenliği bakımından zayıf bir modeldir.

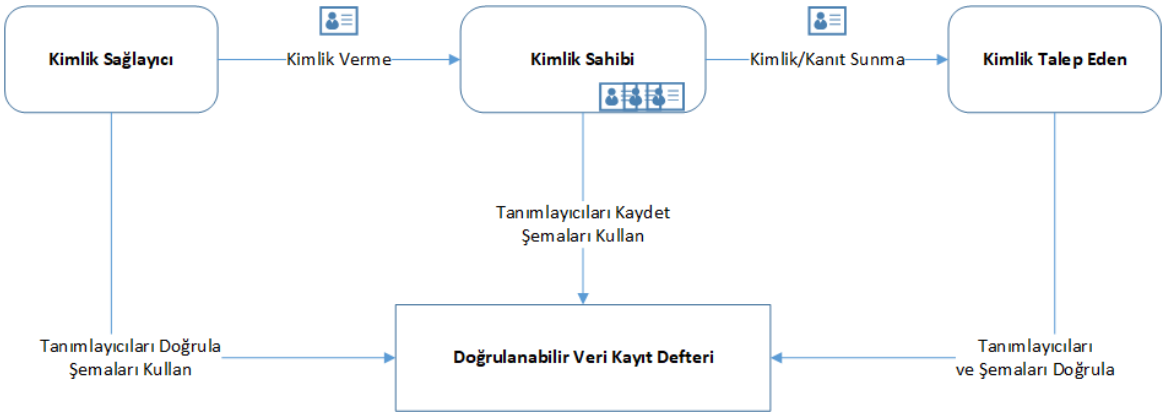
- Federe kimlik yönetim şemasında ise, tek bir merkezi kuruluş yerine birden fazla kuruluş bir araya gelerek belli kurallar çerçevesinde kendi aralarında güven tesis ederler ve her biri kendi kimlik yönetim sistemine sahip olmakla birlikte diğer kuruluşların kimlik yönetim sistemleri ile uyumlu çalışırlar. Federe kimlik yönetim şemasına bir örnek olarak AB üyesi ülkeler "electronic identification and trust services for electronic transactions in the internal market" (eIDAS) adlı yönetmelikle, başka bir ülkenin kendi ulusal kimlik sistemi üzerinden yaptığı kimlik doğrulamasının diğer AB ülkeleri tarafından da geçerli sayılmasını sağlamaktadır (Avrupa Birliği, 2014). Kullanıcı egemenlik bakımından değerlendirildiğinde, federe kimlik yönetim şemasında da kimlik bilgileri ve kimlik paylaşımı konusunda kullanıcı kontrolü az denebilir. Diğer taraftan federe kimlik yönetim şeması için oluşturulması gereken paydaşlar arası güveni sağlamaya yönelik düzenlemelerin ortaya koyulması ve hayata geçirilmesi genellikle zor ve zaman alıcıdır.
- Dağıtık (Kullanıcı egemen) kimlik yönetim şeması, kimliğin asıl sahibi olan kişilerin veya kuruluşların kendi kimlik bilgilerinin saklanmasında, yönetiminde ve paylaşımında kontrol sahibi olduğu modeldir. Bu modelde dijital kimlik verileri kimlik sahibinin kendi dijital cihazlarında verilerini depolayan dijital kimlik cüzdanları ile aracılığıyla tutulur. Dijital kimlik sağlayan yetkili mercilerin verdiği dijital kimlikler bu cüzdanlarda tutularak kimlik sahibinin kimliklerin yönetiminde ve paylaşılmasında tam kontrol sahibi olması sağlanmış olur.

Bu tez çalışmasında önerilen e-ticaret dijital kimlik güven çerçevesi ilkeleri incelendiğinde, en uygun kimlik yönetim şemasının dağıtık veya kullanıcı egemen şeklinde ifade edilen

kimlik yönetim şeması olduğu görülmektedir. Bu model, firmaların kendi dijital kimlikleri ya da dijital kimliklerinde bulunan bilgileri tamamen veya kısmen paylaşma hakkına sahip olmalarına ilişkin ilkeyi sağlayan kimlik yönetim şemasıdır. Bu nedenle bu tez çalışmasında önerilen e-ticaret dijital kimlik güven çerçevesinin yönetim şeması, dağıtık (kullanıcı egemen) kimlik yönetim şeması olarak belirlenmiştir.

4.3. Dijital Kimlik Veri Yapısı

Önerilen güven çerçevesinin en önemli ilkelerinden biri, başka kimlik sistemleri ile de uyumlu bir şekilde çalışabilmeye yönelik olarak uluslararası standartları temel almasıdır. Buna yönelik olarak dijital kimlik bilgilerinin saklanırken ve transfer edilirken kullanılacak veri modeli olarak W3C'nin yayınladığı "Doğrulanabilir Kimlik Veri Modeli" (DKVM) belirlenmiştir (W3C, 2019). Bu veri modeli, dijital kimlikler için şifreleme yöntemleri ile güvenlik mekanizmaları içeren, bilgi gizliliğinin korunmasına olanak sağlayan ve kimlik bilgilerini alan diğer sistemlerin de bu bilgilerin geçerliliğini doğrulayabilmesini sağlayan bir modeldir. "Güven Üçgeni" olarak ifade edilen aşağıdaki şekilde gösterilen bir yapıya dayanmaktadır.



Şekil 4.1. Doğrulanabilir kimlik rolleri ve veri akışı (W3C, 2019)

DKVM yapısında kimlik sağlayıcının kimlik talep eden ile doğrudan bir etkileşimi gerçekleşmez. Bu yapıda kimlik talep eden rolü, kimlik sahibinin kimliğine ilişkin kanıt sunduğu ve bu kanıtın doğrulamasını yapan roldür. Kimlik talep eden doğrulama esnasında da kimlik sağlayıcı ile etkileşime girmez. Doğrulama işlemleri tamamen kimlik sağlayıcının açık anahtarları ve kriptografi teknikleri kullanılarak gerçekleştirilir. Bu nedenle kimlik sağlayıcının kimlik doğrulama işlemini kimlerin yapacağını, yani kimlik talep edenlerin kim olduğunu bilmesine gerek yoktur. Kimlik sahibi ise çeşitli kimlik sağlayıcılardan aldığı

kimliklerdeki bilgileri ayrı ayrı veya seçmeli olarak bir araya getirerek oluşturacağı kimlik kanıtını kimlik talep edenlere ibraz eder. DKVM yapısının sağladığı bu çoklu ilişki yapısı ile İlke 5 sağlanmış olur.

Güven üçgeninde yer alan "Doğrulanabilir Veri Kayıt Defteri" (DVKD) ise kimliklerle ilgili tanımlayıcıları, şemaları ve kimlik sağlayıcıların açık anahtarlarını saklayan güvenilir bir veri deposudur. DVKD güven üçgeninin farklı gerçekleştirimlerinde farklı tekniklerle sağlanabilir. Bu tez çalışmasında önerilen elektronik ticaret güven çerçevesinin güven üçgeni gerçekleştiriminde DVKD bileşeni olarak blok zincirinden faydalanılmıştır. Blok zinciri, güven üçgeni rollerinin saklanan verilere güvenli bir şekilde erişimi için kullanılan dağıtık kayıt defteri olarak kullanılır (W3C, 2019). DVKD olarak kullanılan blok zincirinde dijital kimlikler saklanmaz. Dijital kimlikler, kimlik sahibinin kendi dijital cihazlarında ve dijital cüzdan yazılımlarında saklanır. Blok zinciri kullanımının doğal getirisi olarak DVKD'ye yazılan verilerin daha sonra değiştirilemez olduğu garanti edilmiş olur. Bu sayede İlke 6 sağlanmış olur.

4.4. Güven Çerçevesi Rolleri

Güven üçgeninde yer alan rollerden kimlik sahibi rolü, tüm kimlik yaşam döngüsü işlemlerinin merkezinde yer alır. Potansiyel kimlik sahibi, kendisini veya yetkinliklerine ilişkin özniteliklerini tanımlayan bilgileri içeren bir kimlik almaya ehil olduğunu ispat ettikten sonra yetkili kimlik sağlayıcı tarafından kendisine dijital kimlik verilir. Kimlik sahibi dijital kimliklerinde yer alan bilgi ve özniteliklere ilişkin kanıt sunmak istediğinde, kimliklerindeki bilgilerden oluşturduğu bir kriptografik kanıtı bu kanıtı talep edene gönderir. Kanıtı talep edip kanıtın geçerlilik doğrulamasını gerçekleştiren hizmet sağlayıcısı, kimlik sahibinin beklediği hizmeti sağlar.

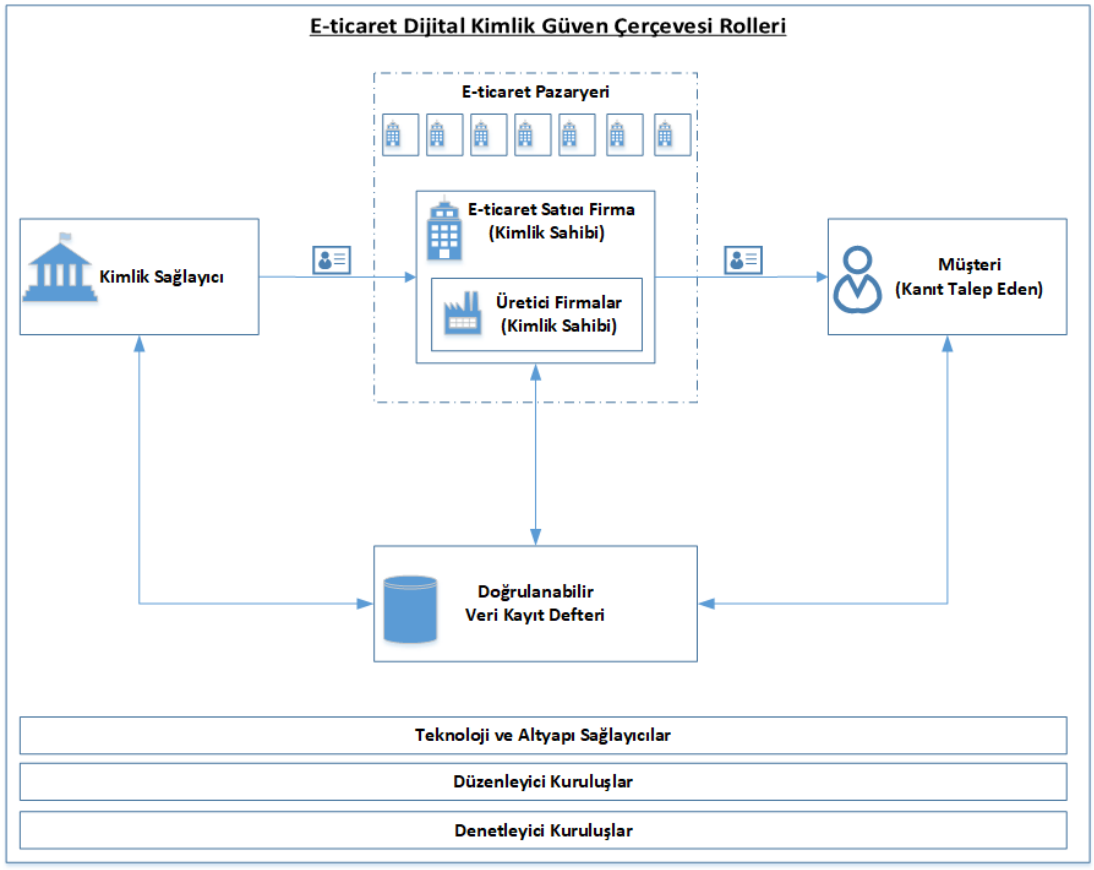
Bu tez kapsamında önerilen güven çerçevesinde, güven üçgenindeki rollere karşılık gelen ve e-ticaret alanına özelleşmiş roller ile birlikte çok daha geniş bir rol kümesi bulunmaktadır. Bu roller aşağıda başlıklar halinde verilmiştir.

- **Müşteriler:** Müşteriler, elektronik ticaretteki potansiyel veya gerçekleşen satın alma işlemine konu mal veya hizmetin alıcı tarafıdır. Güven üçgeninde karşılık gelen rol ise kimlik (kanıt) talep eden rolüdür. Müşteriler, firmaların ibraz ettikleri dijital belgelere

ilişkin kanıtları alıp kendi cihazlarında bulunan dijital cüzdan uygulamasında saklarlar. Bu amaç için özelleştirilmiş dijital cüzdan uygulamaları, blok zincirinden doğrulama için gereken bilgileri çekerek sunulan kanıtların doğrulamasını yaparlar.

- **E-ticaret Firmaları:** E-ticaret firmaları, elektronik ticaretteki satın alma işlemine konu mal veya hizmeti müşteriye sunan taraftır. E-ticaret firmasının güven üçgenindeki karşılığı kimlik sahibi rolüdür. E-ticaret firmaları yetkili kimlik sağlayıcı mercilerden aldıkları kimlik ve belgelere ilişkin kanıtları müşterilere sunarlar.
- **Üretici Firmalar:** Üretici firmalar, elektronik ticaretteki satın alma işlemine konu mal veya hizmeti üreten taraftır. E-ticaret firmalarına benzer şekilde üretici firmalar da güven üçgenindeki kimlik sahibi rolündedir. Üretici firmaların sahip olması beklenen dijital kimlikler, ürüne, üretici firmaya ve üretim yöntemlerine ilişkin verilen dijital belgelerdir.
- **Dijital Kimlik Sağlayıcılar:** Firmalara dijital kimlik vermeye yetkili mercilerdir. Ticari kimlik türündeki dijital kimlikleri bakanlık, vergi dairesi, ticaret odası gibi kurumlar sağlarken firmaların yetkinliklerine ve belli düzenlemelere ve standartlara göre uygunluklarına ilişkin dijital kimlikleri ilgili kuruluşlar sağlamaktadır. Tüm bu kurum ve kuruluşların güven üçgenindeki karşılığı Kimlik Sağlayıcı rolüdür.
- **Teknoloji ve Altyapı Sağlayıcılar:** Dijital kimlik yaşam döngüsü ve güven çerçevesi ile ilgili gerekli her türlü teknoloji ve alt yapıyı sağlayabilen kuruluşlardır. Dijital kimlikler için özelleştirilmiş dijital cüzdanlar ve blok zinciri alt yapıları bu rolün sağlayabileceği hizmetlere örnektir.
- **E-ticaret Pazaryerleri:** Kendi satış platformuna sahip olmayan e-ticaret firmaları için çevrim içi mağazalar ve satış platformu sunarak bu firmaların mal ve hizmetlerini elektronik ticaret ile satabilmelerine olanak sağlayan kuruluşlardır.
- **Düzenleyici Kuruluşlar:** Elektronik ticaret ve dijital kimliklerle ilgili mevzuatı düzenleme yetkisine sahip ulusal ve ulusal veya uluslararası mercilerdir.
- **Denetleyici Kuruluşlar:** Güven çerçevesine katılan tüm rollerin güven çerçevesinde tanımlı düzenlemelere uygunluğunu denetleyen ve uygun davrananlara Güven İşareti veren kuruluşlardır.

Aşağıdaki şekilde dijital kimlik güven çerçevesinin tüm rolleri, rollerin güven çerçevesindeki konumlarını ve birbirleri arasındaki etkileşimi görülmektedir.



Şekil 4.2. E-ticaret dijital kimlik güven çerçevesi rolleri

4.5. Dijital Kimlik Çeşitleri

Bu tez kapsamında önerilen dijital kimlik güven çerçevesi ile iki dijital kimlik çeşidi tanımlanmıştır:

1. Temel dijital kimlikler
2. Bağlamsal dijital kimlikler

Temel dijital kimlikler, firmaların varlığını ve ticari kimliğini gösteren, bu kapsamda bilgiler içeren dijital kimliklerdir. Temel dijital kimlikler firmaların var oluşlarını gösteren kimlikler olduğundan firmaların öncelikle bu türde kimliklere sahip olması gerekir. Bağlamsal dijital kimlikler ise firmaların ürünleri, süreçleri, üretim teknikleri, laboratuvar analizleri, belli standartlara ve düzenlemelere uyumlulukları gibi faaliyet gösterdiği alandaki yetkinliklerini gösteren dijital kimliklerdir. Bu yetkinliklere ilişkin dijital kimlikleri ancak o yetkinliği ölçmeye ve değerlendirmeye yetkili kuruluşlar verebilir.

4.5.1. Temel dijital kimlikler

Firmalarının alabileceği temel dijital kimlik çeşitleri Çizelge 4.1'de verilmiştir.

Çizelge 4.1. Temel dijital kimlikler

Dijital Kimlik Çeşidi	Kimlik Sağlayıcı Kuruluş
Ticari Sicil Kimliği	Ticaret Bakanlığı Ticaret Odaları
Vergi Kimliği	Maliye Bakanlığı Vergi Daireleri
Esnaf/Sanatkâr Sicil Kimliği	Ticaret Bakanlığı Esnaf ve Sanatkâr Odaları

Çizelge 4.1'de verilen temel dijital kimlikler, firmaların kanunen varlığının ispatı olan ve firmayı diğer firmalardan ayıran kimliklerdir. Bu nedenle bu tür dijital kimliklerde o firmaya özel eşsiz bir tanımlayıcı bilgisi, firmanın unvan bilgisi ve adresi yer almalıdır. Çizelge 4.1'de görüldüğü gibi Türkiye'de temel kimlik verebilecek birden fazla türde kuruluş bulunmaktadır. Her bir kuruluşun firmalar için belirlediği eşsiz tanımlayıcı bilgisi de farklı olabilmektedir. Tüm temel dijital kimlik vermeye yetkili kuruluşların sağladıkları kimlik bilgileri incelendiğinde, hepsinde ortak olan eşsiz tanımlayıcının Vergi Kimlik Numarası olduğu görülmektedir. Eşsiz tanımlayıcı bilgi dışında, tüm temel dijital kimliklerde bulunması gereken ortak alanlar da güven çerçevesi kapsamında belirlenmiştir. Belirlenen asgari temel dijital kimliğin güven çerçevesinin dijital kimlik veri yapısı olarak belirlenen DKVM formatında ifade edilmiş hali aşağıdaki gibidir.

```
{
   "@context": [
      "https://www.w3.org/2018/credentials/v1",
      "https://www.ticaret.gov.tr/digital-identity/schemas/v1",
      "https://w3id.org/security/suites/ed25519-2020/v1"
        ],
    "type": ["VerifiableCredential", "TemelKimlik"],
    "issuer": "...",
    "issuanceDate": "...",
    "expirationDate": "...",
    "credentialSubject": {
          "id": "..."
          "kimlik": {
                    "turu": "TemelKimlik",
```

```
                    "unvan": "...",
                    "vergiKimlikNo": "..."
                    "vergiDairesi": "...",
                    "kurulusTarihi": "...",
                    "adres": "...",
                    "sehir": "..."
                }
    },
    "proof": {
        "type": "Ed25519Signature2020",
        "created": "…",
        "verificationMethod”: “…”,
        "proofPurpose": "…",
        "proofValue": "…",
    }
}
```


DKVM formatında gösterilen asgari temel dijital kimlik, tüm temel dijital kimlik sağlayıcıları için minimumda sağlaması gereken alanları göstermektedir. Bu alanların yanında, farklı temel kimlik sağlayıcıların dijital kimliklere ekleyebileceği birçok alan bulunmaktadır. DKVM standardının genişleyebilirlik özelliğinden faydalanılarak, asgari temel dijital kimliğin üzerine inşa edilecek başka temel kimlikler oluşturmak mümkündür. Ticaret Bakanlığı'nın ve ticaret odalarının verebileceği Ticari Sicil Kimliği, asgari temel dijital kimlikteki alanları içeren, bunların üstüne ticari sicil kimliğine özel yeni alanlar ekleyen yeni bir temel dijital kimlik tanımıdır. DKVM'nin bu amaca uygun olarak sağladığı genişleyebilir yapı, "JavaScript Object Notation for Linked Data" (JSON-LD) yöntemine dayanmaktadır. Bu yöntemle, asgari temel dijital kimliğe referans veren ve sadece yeni alanları içeren bir JSON-LD dokümanına ihtiyaç vardır. Kimlik sağlayıcı kuruluşun buna yönelik olarak oluşturacağı JSON-LD dokümanını yayınlaması gerekmektedir. Örneğin Ticaret Bakanlığı aşağıda gösterilen JSON-LD dokümanını https://www.ticaret.gov.tr/digital-identity/contexts/ticarisicil.jsonld gibi bir adreste yayınlayarak asgari temel dijital kimliği nasıl genişlettiğini duyurabilir. Ticari Sicil Kimliği, esas aldığı asgari temel dijital kimliğe yayınladığı bağlam bilgisini ekleyerek aşağıdaki şekilde ifade edilebilir.


```
{
  "@context": {
```

```
    "mersisNo": "https://www.ticaret.gov.tr/digital-identity/schemas/ticariSicil#mersisNo",
    "firmaTuru": "https://www.ticaret.gov.tr/digital-identity/schemas/ticariSicil#firmaTuru",
    "sicilMudurlugu": "https://www.ticaret.gov.tr/digital-identity/schemas/ticariSicil#sicilMudurlugu",
    "firmaDurumu": "https://www.ticaret.gov.tr/digital-identity/schemas/ticariSicil#firmaDurumu",
    "sicilNo": "https://www.ticaret.gov.tr/digital-identity/schemas/ticariSicil#sicilNo",
    "eTebligatAdresi": "https://www.ticaret.gov.tr/digital-identity/schemas/ticariSicil#eTebligatAdresi",
  }
}
```



```
{
   "@context": [
      "https://www.w3.org/2018/credentials/v1",
      "https://www.ticaret.gov.tr/digital-identity/schemas/v1",
      "https://www.ticaret.gov.tr/digital-identity/contexts/ticarisicil.jsonld"
      ],
    "type": ["VerifiableCredential", "TemelKimlik", "TicariSicilKimligi"],
    "issuer": "...",
    "issuanceDate": "...",
    "expirationDate": "...",
    "credentialSubject": {
        "id": "..."
        "kimlik": {
            "turu": "TemelKimlik",
            "unvan": "...",
            "vergiKimlikNo": "..."
            "vergiDairesi": "...",
            "kurulusTarihi": "...",
            "adres": "...",
            "sehir": "...",
            "mersisNo": "...",
            "firmaTuru": "...",
            "sicilMudurlugu": "...",
            "firmaDurumu": "...",
            "sicilNo": "...",
            "eTebligatAdresi": "..."
        }
     },
    "proof": {
         "type": "Ed25519Signature2020",
         "created": "…",
```

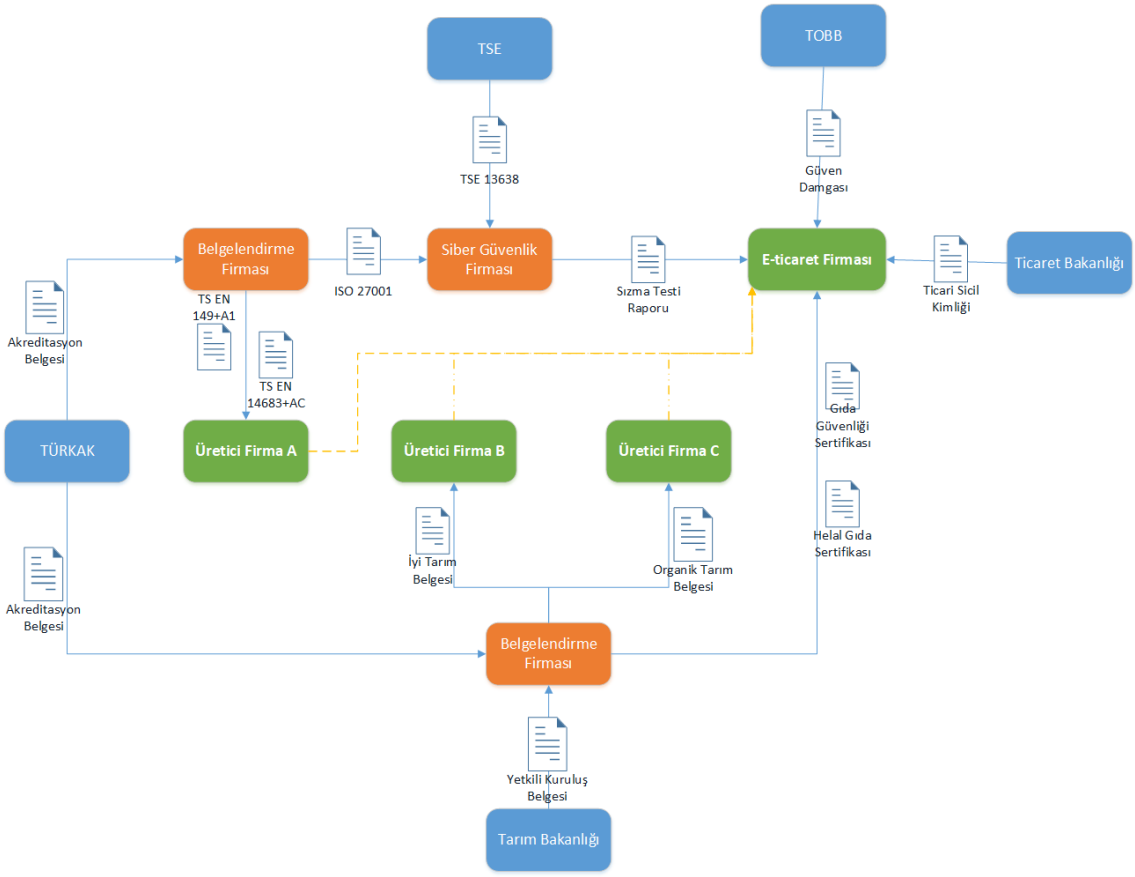
```
        "verificationMethod”: “…”,
        "proofPurpose": "…",
        "proofValue": "…",
    }
}
```


Ticari Sicil Kimliğinde kullanılan genişletme yöntemi kullanılarak diğer kuruluşların sağladığı Vergi Kimliği ve Esnaf/Sanatkâr Sicil Kimliği gibi yeni temel dijital kimlikler tanımlanabilir.

Birden fazla temel dijital kimlik sağlayıcı seçeneğinin bulunması, dijital kimlik güven çerçevesinde yer alan firmaların farklı kimlik sağlayıcılardan farklı temel dijital kimlikler alabileceğini göstermektedir. Hatta aynı firmanın farklı kimlik sağlayıcılardan farklı temel dijital kimlikler alabilmesi de mümkündür. Tüm temel kimlikler için ortak tanımlayıcı bilgisi ile birlikte içermesi gereken asgari alanlar belirlendiğinden, birden fazla temel kimliğe sahip bir firma kimlik talep eden taraflara farklı kuruluşlardan aldığı kimlikleri kanıt olarak sunabilir. Böylelikle güven çerçevesi ilkelerinden İlke 9 sağlanmış olur.

4.5.2. Bağlamsal dijital kimlikler

Firmaların bağlamsal dijital kimlikleri alabilmesi için öncelikle temel dijital kimliklerini almaları gerekir. Çünkü temel dijital kimlikler, firmaların bağlamsal dijital kimliklerini almak için ilgili kuruluşlara sunacakları kimlik kanıtlarıdır. Bağlamsal dijital kimlikler, firmaların faaliyet bağlamına göre, ürünlerine, süreçlerine, üretim tekniklerine, laboratuvar analizlerine, akreditasyon düzenlemelerine, standartlara ve daha birçok sektöre özel uygulamaya göre yetkinliklerini gösteren dijital kimliklerdir. Elektronik ticaret üzerinden satış yapan firmaların sektör ve ürün çeşitliliği dikkate alındığında, Türkiye’de alınabilecek tüm bağlamsal kimliklerin belirlenmesi ve güncel tutulması mümkün görünmemektedir. Bu nedenle, sağlık ve tarım ürünleri alanında faaliyet gösteren varsayımsal bir firma üzerinden örnek bir bağlamsal kimlik akış şeması oluşturulmuştur.



Şekil 4.3. E-ticaret işlemlerine ilişkin örnek bağlamsal dijital kimlikler

Bağlamsal kimlik akış şemasında gösterilen belgeler, Türkiye'deki mevzuata göre farklı sektörlerdeki firmaların alması gereken bazı örnek belgeleri göstermektedir. Elektronik ticaret güven çerçevesi ile bu belgelerin mevzuata uygunluğu koruyacak şekilde dijital ortamda dijital kimlik formatında sağlanması, sunulması ve doğrulanması hedeflenmiştir.

Şekilde gösterilen belgelerden biri olan Güven Damgası, e-ticaret firmalarına faaliyet alanından bağımsız olarak Türkiye Odalar ve Borsalar Birliği (TOBB) tarafından verilir. Güven Damgası, 06/06/2017 tarihinde yayınlanan 30088 sayılı tebliğde yer alan güven damgası alma şartlarını sağlayan firmalara bu şartlara uyduğunun göstergesi olarak verilir (Elektronik Ticarette Güven Damgası Hakkında Tebliğ, 2017). Bu tebliğ ağırlıklı olarak e-ticaret firmalarının güvenlikle ve sundukları mal ve hizmetlerle ilgili şartları düzenler. Şekildeki akış incelendiğinde, Güven Damgası alabilmek için ön koşul olarak başka birçok belgenin alınması gerektiği görülmektedir. Bunlardan ilki, e-ticaret firmasının Ticaret Bakanlığı veya benzeri temel kimlik sağlayıcı kuruluşlardan temel kimlik alması gerekmektedir. Yine e-ticaret firmasının, yetkilendirilmiş bir sızma testi hizmeti veren firmadan sızma testi hizmeti alması ve bu testin sonucunda başarılı bir sızma testi raporu

alabilmesi gerekmektedir. Bir siber güvenlik firmasının sızma testi için yetkilendirilmesi için ise, o firmanın TSE'den Onaylı Sızma Testi Firması olarak akredite olması ve TSE 13638 belgesi almış olması gerekmektedir. Siber güvenlik firmasının da TSE'den bu belgeyi almadan önce alması gereken ISO 27001 Bilgi Güvenliği Yönetim Sistemi belgesi şartı bulunmaktadır. ISO 27001 belgesini verebilen firma, önceden TÜRKAK tarafından akredite edilmiş olmalıdır.

Şekilde gösterilen bir diğer belge türü de tarımsal üretim yapan firmalara yetkili belgelendirme firmaları tarafından verilen organik tarım ve iyi tarım belgeleridir. Bu belgeleri vermeye yetkili belgelendirme firmaları Tarım Bakanlığının yetkilendirdiği ve bakanlığın şartlarını sağlayan firmalardır. Sağlık ürünleri sektöründeki üretici firmalara yönelik olarak ise bazı belgelendirme kuruluşları tarafından, N95 ve cerrahi maske gibi ürünler için CE belgesi uyumluluğu kapsamında TS EN 149+A1 ve TS EN 14683+AC standartlarına uygunluk testleri yapılabilmektedir. Bu belgelendirme kuruluşlarının da bu testleri yapabilmek için TÜRKAK'tan akredite olması gerekir. Benzer şekilde, TÜRKAK akreditasyonu ile bazı belgelendirme kuruluşları Gıda Güvenliği Sertifikası ve Helal Gıda Sertifikası verebilmektedir.

Şekilde gösterilen örnek bağlamsal dijital kimlikler için dijital kimlik çeşidi, kimlik sahibi ve kimlik sağlayıcı Çizelge 4.2.'de verilmiştir.

Çizelge 4.2. E-ticaret işlemlerine ilişkin örnek bağlamsal dijital kimlikler

Dijital Kimlik Çeşidi	Kimlik Sahibi	Kimlik Sağlayıcı
Güven Damgası	E-ticaret Firması	Türkiye Odalar ve Borsalar Birliği
Sızma Testi Raporu	E-ticaret Firması	Siber Güvenlik Firması
TSE 13638 - Sızma testi yapan personel ve firmalar için şartlar	Siber Güvenlik Firması	TSE
ISO 27001 - Bilgi Güvenliği Yönetim Sistemi	Siber Güvenlik Firması	Belgelendirme Kuruluşu
TÜRKAK Akreditasyon Belgesi	Belgelendirme Kuruluşu	TÜRKAK
Tarım Bakanlığı Yetkili Kuruluş Belgesi	Belgelendirme Kuruluşu	Tarım Bakanlığı
Organik Tarım Sertifikası	Üretici Firma	Belgelendirme Kuruluşu
İyi Tarım Uygulamaları Sertifikası	Üretici Firma	Belgelendirme Kuruluşu
TS EN 149+A1 - Parçacıklara karşı koruma amaçlı filtreli yarım maskeler - Özellikler, deneyler ve işaretleme	Üretici Firma	Belgelendirme Kuruluşu
TS EN 14683+AC - Tıbbi yüz maskeleri – Gereklilikler ve deney yöntemleri	Üretici Firma	Belgelendirme Kuruluşu
ISO 22000 - Gıda Güvenliği Yönetim Sistemi	E-ticaret Firması/ Üretici Firma	Belgelendirme Kuruluşu
TS OIC/SMIIC 1: 2011 Helal Gıda Genel Kılavuzu Standardı	E-ticaret Firması/ Üretici Firma	Belgelendirme Kuruluşu

Tıpkı temel dijital kimlikler gibi bağlamsal dijital kimlikler de DKVM formatında ifade edilebilir. TOBB'un sağladığı güven damgası belgesinin DKVM formatında JSON olarak gösterimi aşağıda verilmiştir.


```
{
   "@context": [
      "https://www.w3.org/2018/credentials/v1",
      "https://www.tobb.org.tr/digital-identity/schemas/v1",
      "https://w3id.org/security/suites/ed25519-2020/v1"
       ],
    "type": ["VerifiableCredential", "BaglamsalKimlik", "GuvenDamgasi"],
    "issuer": "...",
    "issuanceDate": "...",
    "expirationDate": "...",
    "credentialSubject": {
          "id": "...",
          "kimlik": {
                    "turu": " GuvenDamgasi",
                    "unvan": "...",
                    "sektor": "..."
                    "mersisNo": "...",
                    "guvenDamgasiSicilNo": "...",
                }
    },
    "proof": {
          "type": "Ed25519Signature2020",
          "created": "…",
          "verificationMethod": "…",
          "proofPurpose": "…",
          "proofValue": "…",
    }
}
```


4.6. Kimlik İspatı ve Dijital Kimlik Alma

Dijital kimlik sağlayıcının bir firmaya dijital kimlik verebilmesi için öncelikle firmanın kim olduğunu veya dijital kimliğin bağlamında yer alan yetkinliklere sahip olduğunu, diğer bir ifadeyle talep ettiği dijital kimliği almaya muvafık olduğunu kimlik sağlayıcıya ispatlaması gerekmektedir. Firma bir tüzel kişilik olduğundan, bu süreç hem firmanın tüzel kişilik olarak

ispat sunmasını hem de firma yetkilisinin gerçek kişi olarak kimliğini ve firma yetkili olduğunu ispatlamasını gerektirir. Dijital kimlik almanın ön şartı olan tüm bu kimlik ve yetkinlik kanıtlama aşamalarının farklı yöntemlerle gerçekleştirilmesi mümkün olduğundan farklı yöntemlerin farklı güvence seviyeleri olması kaçınılmazdır. Güvence seviyesini etkileyen bir diğer faktör de kimlik sağlayıcının "sorumlu yetkili kuruluş", yani konuya ilişkin yasal düzenlemelerde kimlik bilgilerinin saklanması ve yönetimi için yetkilendirilmiş yasal merci olup olmamasıdır. Firmaların ticari sicilleriyle ilgili işlemlerden sorumlu kuruluş yasa gereği firmanın bağlı bulunduğu ticaret odası olduğundan, ticari sicil kimliği için sorumlu yetkili kuruluş ticaret odaları olarak kabul edilebilir. Bir firmaya ticari sicil kimliğini o bilgilere dolaylı olarak sahip ticaret odası dışında bankalar gibi başka kuruluşların da vermesi mümkündür. Fakat bu durumda kimlik sağlayıcı sorumlu yetkili kuruluş olmadığından güvence seviyesi daha düşük olacaktır. Bu çalışmada önerilen dijital kimlik güven çerçevesi ile farklı kimlik ispatı yöntemlerine ve sorumlu yetkili kuruluş durumlarına göre farklı güvence seviyeleri olabileceği değerlendirilmiş ve en yüksek güvence seviyesini sağlayacak kimlik ispatı yöntemi seçilmiştir. Seçilen yönteme göre e-ticaret firmasının sorumlusunun kimlik ispatı Elektronik Kimlik Doğrulama Sistemi (EKDS) kullanılarak yapılmalı ve dijital kimliği sağlayacak olan kuruluş sorumlu yetkili kuruluş olmalıdır. Önerilen güven çerçevesi kapsamında belirlenen kimlik ispatı için kullanılacak yöntem ve güvence seviyesi, güven çerçevesi ilkelerinden İlke 2'nin karşılanmasını sağlar.

EKDS, yeni nesil çipli kimlik kartlarının ve biyometrik verilerin kullanılmasıyla kimlik ispatı sağlayan ve çeşitli güvenlik mekanizmaları içeren TÜBİTAK BİLGEM'in geliştirdiği bir sistemdir. EKDS aracılığıyla kimlik doğrulaması yapıldığında (UEKAE, 2015):

- Kullanılan kimliğin NVİGM tarafından verilen bir kimlik olduğunu,
- EKDS'de kimliği doğrulanan kişinin fiziki olarak doğrulama yapılan yerde bulunan, kimlik kartını ibraz eden ve kimlik kartının sahibi kişi olduğunu,
- Doğrulamanın yapıldığı zaman, yer ve doğrulama sebebi bilgilerinin alınmasını sağlar.

Kimlik doğrulamada yasal olarak EKDS'nin kullanılmasına yönelik mevzuat, 2020 yılında çıkarılan bir yönetmelikle düzenlenmiştir. (Türkiye Cumhuriyeti Kimlik Kartı Elektronik Kimlik Doğrulama Sistemi Yönetmeliği, 2020). Mevzuat, EKDS ile kullanılabilecek on bir farklı seviyede kimlik doğrulama yöntemi belirlemiş, her bir yöntemin hangi güvenlik

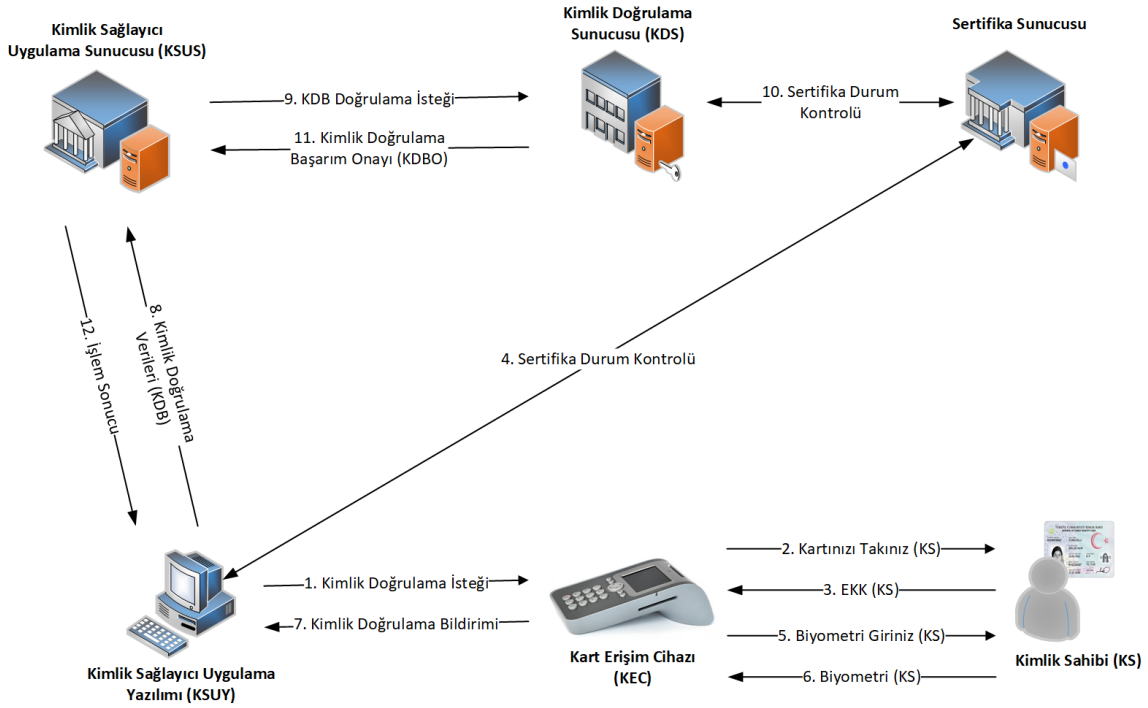
önlemlerini ve kart erişim cihazı (KEC) türünü içerdiğini tanımlamıştır. EKDS kimlik doğrulama yöntemleri özet olarak EKDS web sitesinde de açıklanmıştır (UEKAE, 2015).

Y1'den Y11'e kadar adlandırılan EKDS'de tanımlı on bir kimlik doğrulama yönteminden en fazla güvenlik sağlayan yöntem Y11 yöntemidir. Bu nedenle bu tez çalışmasında önerilen güven çerçevesinin kimlik ispatı yöntemi olarak Y11 belirlenmiştir. Bu yöntem, öncelikle kimlik kartı ile KEC arasında bir doğrulama gerçekleştirerek güvenli mesajlaşma sağlar. Daha sonra kimlikte yüklü olan kimlik doğrulama sertifikasının geçerliliği sertifika sunucusu üzerinden doğrulanır. Bu iki aşamadan sonra kart sahibinin başvuruyu yapan kişi olduğunun doğrulaması PIN, biyometrik veri ve fotoğraf kullanılarak yapılır.

TSE tarafından yayınlanan EKDS standartlarında, on bir kimlik doğrulama yöntemi dışında ayrıca kimlik doğrulama süreçleri de tanımlanmıştır (TSE, 2017). Bu süreçler aşağıdaki değişkenlere göre birbirinden ayrılmaktadır:

- Süreçte yer alan KEC türü,
- Süreçte Kimlik Doğrulama Politika Sunucusu (KDPS) yer alıp almadığı
- Süreçte kimlik tespiti yapan kişinin yer alıp almadığı

Aşağıdaki şekil, bu süreçlerden, güven çerçevesi için seçilen Y11 kimlik doğrulama yöntemini destekleyen örnek bir süreci göstermektedir. Gösterilen süreçteki KEC, kimlik kartı ve biyometrik doğrulamayı destekleyen ve USB üzerinden haberleşme sağlayan bir cihazdır. Ayrıca bu süreçte kimlik doğrulama için KDPS ve kimlik tespitini yapan kişi yer almamaktadır.

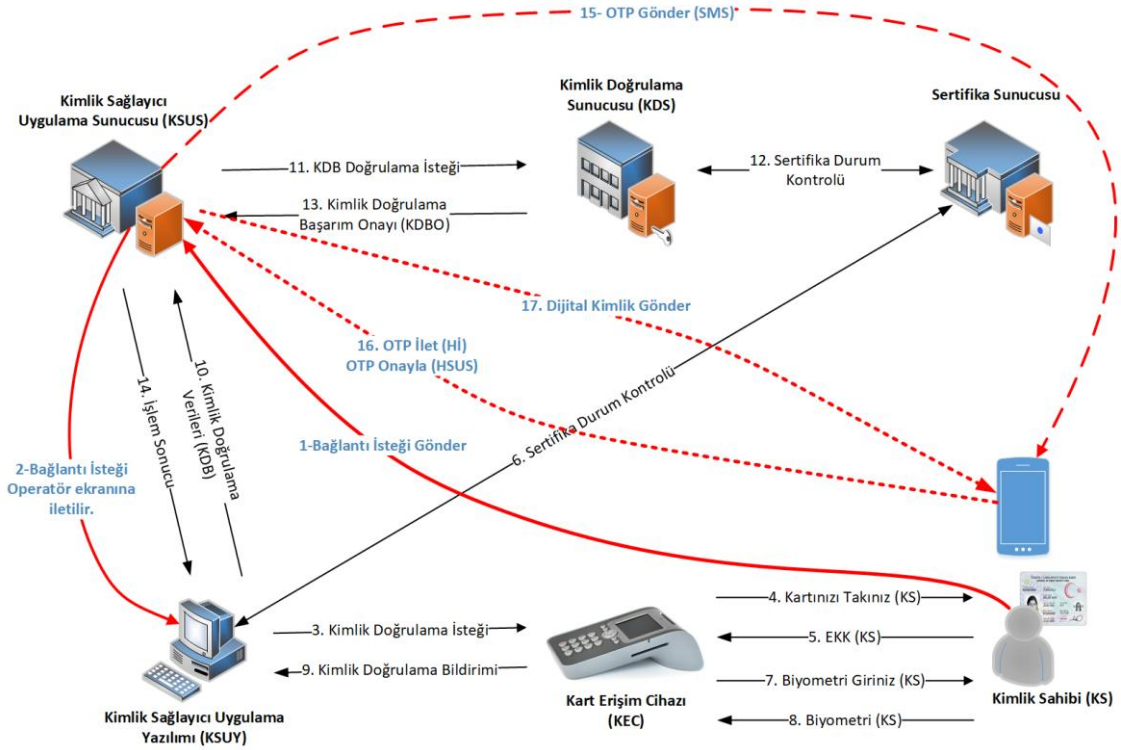


Şekil 4.4. EKDS kimlik doğrulama örnek süreci (TSE, 2017)

E-ticaret dijital kimlik güven çerçevesinde yer alan firmalar kimlik ispatını EKDS üzerinden yaptıklarında, firmaların başvuruyu yapan yetkilileri EKDS'de Kimlik Sahibi (KS) rolünde olacaklardır. EKDS üzerinden yürütülen kimlik ispatı süreci ile firma yetkilisine ilişkin aşağıdaki doğrulamaların güvenli bir şekilde yapılması sağlanmış olacaktır:

- Firma yetkilisinin geçerli bir T.C. kimlik kartına sahip olduğu ve doğrulamanın bu kartla yapıldığı (KEC ile kimlik kartı doğrulama)
- Sunulan kimlik kartının firma yetkilisine ait olduğu (Biyometri doğrulama)
- Firma yetkilisinin fiziken kimlik doğrulamanın yapıldığı yerde bulunduğu (KEC ile kimlik kartı doğrulama ve Biyometri doğrulama)

Yukarıda gösterilen süreç, sadece EKDS ile kimlik doğrulama aşamalarını içermektedir. Güven çerçevesi kapsamında bu süreçteki asıl amaç, firma yetkilisinin kimlik doğrulaması yapıldıktan sonra firmaya bir dijital kimlik vermektir. EKDS ile firma yetkilisinin kimliğinin doğrulanması süreci bu çalışma kapsamında genişletilerek sürecin dijital kimlik verme aşamalarını da içermesi sağlanmıştır. Bu sürecin gerçekleştirilmesi için hizmet veren rolünde ilgili dijital kimliği vermeye yetkili bir kuruluş, örneğin ticaret odası yer almalıdır. EKDS sürecinin dijital kimlik alma aşamaları ile genişletilmiş hali aşağıdaki şekilde gösterilmiştir.



Şekil 4.5. EKDS doğrulaması ile dijital kimlik alma

4.7. Dijital Kimlik İbrazı ve Doğrulama

Dijital kimlik ibrazı, kimlik sahiplerinin sahip oldukları dijital kimliklerini hizmet almak istedikleri tarafların talep etmesi durumunda kanıt olarak sunmaları işlemidir. Talep eden taraf kimlik sahibinin sunduğu dijital kimlik kanıtlarını doğruladıktan sonra kimlik sahibinin beklediği hizmeti sunar. Güven çerçevesi kapsamında ise, yetkili kuruluşlardan dijital kimlik almış olan e-ticaret firmaları veya üretici firmalar, alıcılar talep ettiğinde bu dijital kimliklerini ispat eden kanıtları alıcılara ibraz ederler. Kullanıcı egemen kimlik yönetim şemasına göre firmalar dijital kimliklerini kendi dijital cüzdanlarında saklarlar ve talep edilmesi durumunda dijital kimlik bilgilerinden kanıt üreterek bu kanıtları ibraz ederler. Dijital cüzdanlar, elektronik olarak imzalanmış olan doğrulanabilir kimlikleri saklayabilen yapılardır (Nitin ve Jenkins, 2020).

Firmaların kimlik kanıtı ibrazından sonraki aşama, kimlik kanıtını alan alıcıların bu kanıtı doğrulamasıdır. Dijital kimlik güven çerçevesinde bu doğrulama işlemi, alıcının blok zincirinden alacağı doğrulama için gerekli kimlik sağlayıcı açık anahtarları ve kimlik tanımları ile yapılır. Dijital kimlik güven çerçevesinde dijital kimliklerin veri yapısı olarak

belirlenen DKVM'ye göre firmaların sahip oldukları dijital kimlikler ile alıcılara sundukları kimlik kanıtları farklı veri yapılarıdır. Alıcılara sunulan kimlik kanıtları, farklı dijital kimliklerden seçilen farklı özniteliklerin birleşiminden de oluşabilen, dijital kimliklerle birebir aynı olmak zorunda olmayan Doğrulanabilir İbraz (Verifiable Presentation) olarak tanımlanır. Örneğin firma temel dijital kimliğinden unvan ve kurulusTarihi bilgisini, güven damgası kimliğinden de guvenDamgasiSicilNo bilgisini bir araya getirerek yeni bir Doğrulanabilir İbraz oluşturabilir ve bunu alıcıya ibraz edebilir. Bu örnekteki Doğrulanabilir İbraz aşağıdaki şekilde ifade edilebilir.


```
{
   "@context": [
      "https://www.w3.org/2018/credentials/v1",
      "https://www.ticaret.gov.tr/digital-identity/schemas/v1",
      "https://www.tobb.org.tr/digital-identity/schemas/v1"
   ],
   "type": "VerifiablePresentation",
   "verifiableCredential": [
   {
      "@context": [
         "https://www.w3.org/2018/credentials/v1",
         "https://www.ticaret.gov.tr/digital-identity/schemas/v1"
      ],
      "type": ["VerifiableCredential", "TemelKimlik", "TicariSicilKimligi"],
      "credentialSchema": {
         "id": "...",
         "type": "..."
       },
   "issuer": "...",
   "credentialSubject": {
      "unvan": "...",
      "kurulusTarihi": "..."
      },
   "proof": {
      "type": "AnonCredDerivedCredentialv1",
      "primaryProof": "...",
      "nonRevocationProof": "..."
      }
   },
   {
```

```
        "@context": [
            "https://www.w3.org/2018/credentials/v1",
            "https://www.tobb.org.tr/digital-identity/schemas/v1"
        ],
        "type": ["VerifiableCredential", "BaglamsalKimlik", "GuvenDamgasi"],
        "credentialSchema": {
            "id": "...",
            "type": "..."
        },
        "issuer": "...",
        "credentialSubject": {
            "guvenDamgasiSicilNo": "..."
        },
    "proof": {
        "type": "AnonCredDerivedCredentialv1",
        "primaryProof": "...",
        "nonRevocationProof": "..."
        }
  }],
    "proof": {
        "type": "AnonCredPresentationProofv1",
        "proofValue": "..."
    }
}
```


Doğrulanabilir ibrazlar, doğrulanabilir kimliklerden üretilen, bir veya daha fazla kimlikten seçilen özniteliklerin bir araya getirilmesiyle oluşturulan, böylelikle ibraz edilecek bilgilerin kontrolünün kimlik sahibinde olmasını sağlayan bir mekanizmadır. Kimlik sahibine kimlik bilgilerinin paylaşımının tam kontrolünü veren bu yapı ile İlke 3 karşılanmış olur.

4.8. Güven İşareti

Güven işareti, dijital kimlik güven çerçevesine katılan firmaların bu çerçeve kapsamında belirlenen kurallara ve düzenlemelere uygun olarak hareket ettiklerini gösteren bir belirteçtir. Güven çerçevesinde yer alan değerlendirme ve denetleme kuruluşları aracılığıyla firmaların güven çerçevesine uyumluluk kontrolleri yapılarak firmalara güven işareti verilir. Denetim sonucunda güven çerçevesi kurallarına ve düzenlemelerine aykırı hareket ettiği

tespit edilen firmaların güven işareti almasına izin verilmez. Güven işareti ve ilgili kontrol ve denetimler ile güven çerçevesi ilkelerinden İlke 8 karşılanmış olur.

2017 yılından beri ülkemizde uygulanan güven damgası, güven işaretine benzer bir amaca hizmet etmektedir. Güven damgası da güven işareti gibi ilgili firmanın belli şartları taşıdığının göstergesidir ve e-ticarette güveni artırmaya yönelik bir uygulamadır. Fakat güven damgası çok dar bir kapsamda uyulması gereken şartlar içermekte, firmanın sadece bir kısım siber güvenlik önlemlerine sahip olduğunu ve e-ticaret hizmetlerini birtakım kurallar çerçevesinde yürüttüğünü göstermektedir. Türkiye'de güven damgasını vermek için tek yetkilendirilmiş kuruluş TOBB'dur. TOBB'un güven damgası için oluşturduğu internet sitesinde "güven damgasının işlevi açık bir şekilde asgari güvenlik ve hizmet kalitesi standardının varlığına işarettir" şeklinde ifade edilmiştir (TOBB, 2018). Güven damgasına sahip e-ticaret firmaları aşağıdaki şekilde gösterilen işareti sitelerinde bulundururlar.



Şekil 4.6. Güven damgası

Önerilen dijital kimlik güven çerçevesindeki güven işareti ise güven damgasına göre çok daha geniş kapsamlı kural ve düzenlemelere uyumluluğu gösteren bir işarettir. Güven damgası, güven çerçevesi kapsamında değerlendirilebilecek birçok dijital kimlik türünden yalnızca biri olarak değerlendirilebilir. Dijital kimlik güven çerçevesi kapsamında bir firmanın güven işaretine sahip olması, birçok başka uyumluluk ile birlikte güven damgası şartlarını da taşıdığını göstermektedir. Aynı zamanda güven çerçevesinde yer alan dijital kimlik alma, kanıt ibrazı ve kanıt doğrulama aşamalarının güven damgası için de doğal olarak uygulamasını sağlayacaktır.

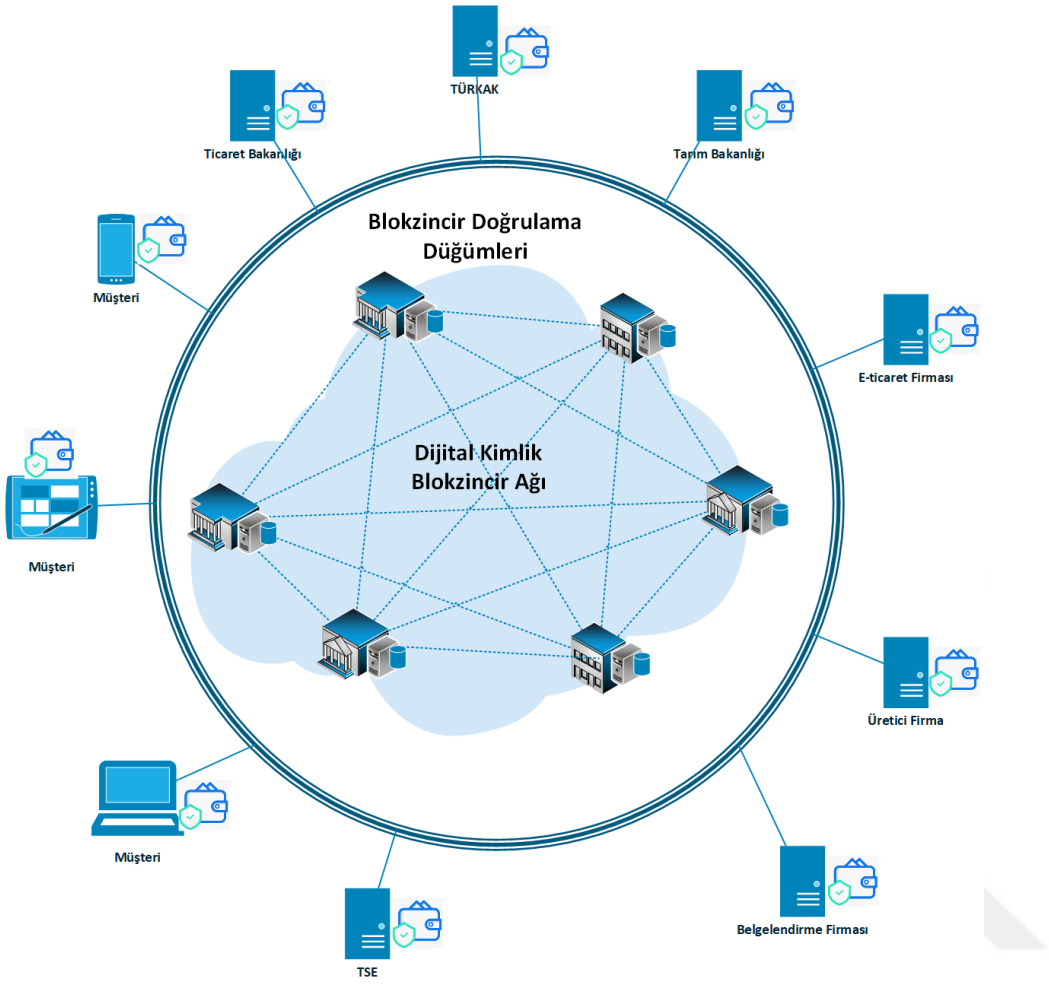
4.9. Güven Çerçevesi Paydaşları ve Yönetişimi

E-ticaret dijital kimlik güven çerçevesini oluşturan paydaşlar güven çerçevesi mimarisindeki konumları bakımından iki ana tabakada incelenebilir.

1. Blok Zinciri Ağını Oluşturan Paydaşlar
2. Blok Zinciri Ağıyla Haberleşen Paydaşlar

Şekil 4.7'de gösterilen bu iki tabakadan ilki, güven çerçevesi mimarisinin merkezinde bulunan dijital kimlik blok zinciri ağıdır. Bu ağı oluşturan paydaşlar, e-ticaret dijital kimlik güven çerçevesindeki rolünden bağımsız olarak blok zinciri ağını oluşturmak amacıyla blok zinciri düğümü olarak görev yaparlar. Hatta blok zinciri düğümlerinin güven çerçevesinde başka bir rolü olmayan paydaşlar olması bile mümkündür. Örneğin e-ticaret ekosisteminde doğrudan bir rolü olmayan TUBİTAK gibi kuruluşlar da blok zinciri ağının oluşturulması için blok zinciri düğümü olarak görev yapabilirler. Blok zinciri verileri her bir blok zinciri düğümünde değiştirilemez şekilde dağıtık olarak tutulduğundan veri bütünlüğü garanti edilmiş olur. E-ticaret dijital kimlik güven çerçevesinin kimlik yönetim şeması olan kullanıcı egemen kimlik şeması gereği blok zinciri düğümlerinde dijital kimliklerin kendisi saklanmaz. Bu dijital kimlikleri tanımlamak ve doğrulamak için gerekli olan kimlik şemaları, kimlik tanımları ve kimlik sağlayıcı açık anahtarları blok zinciri ağında tutulur. E-ticaret güven çerçevesinde dijital kimlik yaşam döngüsünde yer alan tüm rollerin blok zincirinde saklanan bu verilere erişmesi gerektiğinden ve saklanan veriler hassas veriler olmadığından blok zinciri ağından okuma işlemleri izne tabi değildir. Fakat bu verilerin blok zinciri ağına yazılması için bu verileri yazacak olan dijital kimlik sağlayıcı kuruluşların ağa bu yetkiyle dahil olabilmek için izin almaları gerekmektedir. Bu nedenle önerilen dijital kimlik güven çerçevesinde yer alacak blok zinciri "Kısmen İzin Gerektirmeyen Blok Zinciri Ağı" olmalıdır (Usta ve Doğantekin, 2019).

Şekil 4.7'de gösterilen iki tabakadan merkez tabakayı çevreleyen dış tabaka, merkezde bulunan blok zinciri ağı ile etkileşimde bulunan dijital cüzden sahibi istemcilerden oluşur. Blok zinciri ağı ile haberleşen istemciler, güven çerçevesinde tanımlı rolleri olan kimlik sağlayıcılar, kimlik sahipleri ve kimlik/kanıt talep edenlerdir. Bu rollere yasal olarak yetkilendirilmiş bakanlık, ticaret odası, belgelendirme kuruluşu, TÜRKAK gibi kimlik sağlayıcı kuruluşlar, e-ticaret firması, üretici firma, siber güvenlik firması gibi kimlik sahibi firmalar ve firmalardan kimlik kanıtı talep eden bunları blok zinciri ağı yardımıyla doğrulayan müşteriler dahildir.



Şekil 4.7. Blok zinciri tabanlı dijital kimlik mimarisi

Dış katmanda yer alan paydaşların teknolojik alt yapı olarak tek ihtiyacı dijital kimliklerini saklayabilmek ve blok zinciri ağıyla haberleşebilmek için gerekli olan dijital cüzdan uygulamalarıdır. Bu nedenle dış katman paydaşlarının sisteme dahil olması ve sistemden ayrılması kolaydır. Fakat iç katmanda yer alan blok zinciri ağını oluşturan blok zinciri düğümü görevi yapan paydaşların ağın oluşturulması ve sürdürülebilmesi için hem sunucu kaynağı hem de teknik personel kaynağı ayırması gerekir. Bu nedenle blok zinciri ağını oluşturan paydaşların sayısının sık değişmesi beklenmez. Blok zinciri ağının güvenilir olması ve ağa gelen istek miktarına göre ortaya çıkabilecek yükü karşılayabilmesi için asgari sayıda blok zinciri düğümüne ihtiyaç vardır.

E-ticaret dijital kimlik güven çerçevesinin yönetişiminde görev alacak paydaşların ağırlıklı olarak blok zinciri ağını oluşturan ve bu konuda yatırım yapan paydaşlar olması beklenir. Blok zinciri ağı ve güven çerçevesi konusunda alınacak kararlar ve uygulamalar konusunda bu paydaşların oluşturacağı bir koordinasyon kurulunun görev yapması önerilmektedir. Blok

zinciri ağının yönetimi ve genişlemesine ilişkin kurallar ve e-ticaret dijital kimlik güven çerçevesi kapsamında alınacak kararlar koordinasyon kurulu tarafından belirlenmelidir. Koordinasyon kurulunun e-ticaret dijital kimlik güven çerçevesindeki rollerin dengeli bir biçimde temsil edileceği ve belli bir rolün ağır basmayacağı bir kurul olması temsil adaleti bakımından önemlidir. E-ticaret konusunda en yetkili devlet kurumu olan Ticaret Bakanlığı, kamu kurumları ile e-ticaret sektörü arasında bir köprü görevi yapan TOBB, ana dijital kimlik sağlayıcılardan olan TSE ve TÜRKAK, belgelendirme kuruluşları, e-ticaret pazar yerleri, satıcı firmalar, e-ticaret dernekleri gibi paydaşların bu kurulda temsil edilmesi, alınacak kararların tüm paydaşlar açısından değerlendirilmesini ve tüm paydaşların güven çerçevesinde alınan kararların bir parçası olmasını sağlayacaktır. Güven çerçevesinin yönetişiminin farklı rollerdeki paydaşlardan ortak oluşturulmuş bir kurul tarafından sağlanması, güven çerçevesinin kurallarının ve süreçlerinin de şeffaf bir şekilde ilgili tüm paydaşlara açık olmasını sağlayacaktır. Bu şeffaflık ile güven çerçevesi ilkelerinden İlke 7 gerçekleştirilmiş olur. Koordinasyon kurulunun aşağıdaki konularda kararlar alması ve düzenlemeler yapması beklenebilir:

- Blok zinciri ağına katılım için sağlanması gereken şartlar ve katılım prosedürü,
- Blok zinciri ağına yeni katılacak üyelerin sağlayacağı teknik alt yapı, sunucu ve insan kaynağı ile hizmet seviyesi taahhütleri,
- Güven çerçevesinde dijital kimlik sağlayıcısı olarak yer alacak yasal yetkili mercilerin ağa katılım esnasında doğrulanmalarına ilişkin prosedürler,
- Dijital kimlik sağlayıcısı olarak yer alacak yasal yetkili mercilerin uyması gereken kurallar,
- Blok zinciri ağından faydalanacak paydaşlar için belirlenecek hizmet ücretleri,
- Farklı kimlik sağlayıcıların verdiği dijital kimliklerin ortaklanması amacıyla dijital kimlik türleri için asgari dijital kimlik yapılarının oluşturulması.

Güven çerçevesinde yer alan kuruluşların yanı sıra kanıt talep eden rolündeki e-ticaret müşterileri de güven çerçevesinin kurallarına uymalıdırlar. E-ticaret firmalarından kanıt talep eden müşteriler, firmalara ilişkin doğrulanabilir ibraz yoluyla aldıkları bilgileri sadece dijital cüzdan aracılığıyla doğrulayarak firmaların güvenilirliği hakkında fikir edinebilmek için kullanmalıdırlar. Firmalara ilişkin bilgileri başka bir amaçla kullanmamalıdır. Güven çerçevesi hizmetlerinden faydalanacak olan müşterilerin öncelikle güven çerçevesi

kurallarını kabul ettiklerine dair elektronik rıza alınmalıdır. Böylelikle güven çerçevesi ilkelerinden İlke 4 gerçekleştirilmiş olur.

5. BLOK ZİNCİRİ TEMELLİ E-TİCARET İTİBAR SİSTEMİ

Modelimizin ana hedefleri, e-ticaret ekosistemindeki alıcıların sağladığı dürüst geri bildirimleri en üst düzeye çıkarmak, yanıltıcı ve taraflı geri bildirimleri en aza indirmek ve itibar sistemine yönelik bazı temel saldırıları önleyerek dolandırıcılık faaliyetlerini en aza indirmektir. Modelimizin ilkeleri bu hedefler etrafında oluşturulmuştur.

Chang ve arkadaşları yaptıkları araştırmada, itibar sistemlerinde dürüst geri bildirimleri artırmaya yönelik yaklaşımları iki ana kategoride sınıflandırmıştır (Chang, Xiao ve Xu, 2019):

1. Geri bildirim verenlerin mahremiyetini korumak,
2. Geri bildirim verenlere teşvik sağlamak

Tez çalışması kapsamında önerilen itibar sistemi modeli, alıcılardan dürüst geri bildirim almaya yönelik olarak bahsedilen iki yaklaşımı dikkate alarak tasarlanmıştır.

5.1. Modelin Prensipleri

Modelin belirlenen hedeflerine ulaşması için aşağıdaki prensiplerin modele temel teşkil etmesi gerektiği sonucuna varılmıştır.

- Satıcılar, kullandıkları e-ticaret platformu ne olursa olsun ve daha önce kayıt yaptırıp yaptırmadıklarına bakılmaksızın, benzersiz ve global olarak tanımlanmalı ve sisteme kaydedilmelidir.
- Sistem, geri bildirim veren alıcıların mahremiyetini korumalıdır. Bir satıcı için geri bildirimi kimin sağladığı bilgisinin ortaya çıkarılması mümkün olmamalıdır. Bu nedenle sistem, geri bildirim ile geri bildirimin sahibi arasında herhangi bir bağlantı kurmamalıdır.
- Sistem, geri bildirim veren alıcıların mahremiyetini korurken, satın alma işlemi gerçekleştirmeyen hiç kimsenin bir satıcı için geri bildirim göndermesine izin vermemelidir. Bu nedenle, sistem yalnızca tamamlanan satın alma işlemleriyle bağlantılı geri bildirimlere izin vermelidir. Ayrıca sistem, tek bir satın alma işlemi için birden fazla geri bildirim gönderilmesini engellemelidir.

- Geri bildirim gönderme izinleri, yalnızca e-ticaret faaliyeti tamamlandıktan sonra belirli bir süre için geçerli olmalıdır. Başka bir deyişle, izinlerin geçerliliklerinin bir sona erme tarihi olmalıdır.
- Alıcılar, satıcılar için geri bildirim sağlamaya teşvik edilmelidir. Sistem satıcıların kendi platformlarında olan teşvik mekanizmaları ile entegrasyonu desteklemelidir.

5.2. Model Mimarisi

İtibar sistemimiz aşağıdaki varlıkları içermektedir:

Alıcı: Alıcı ***A***, bir e-ticaret işleminde satıcı ***S***'den mal veya hizmet satın alan varlıktır. ***A***, satın alma işleminden en üst seviyede faydayı ve memnuniyeti elde etmek ister. Bu nedenle, ***A***'nın satın alma işleminden önce ***S*** ile ilgili diğer alıcıların verdiği yorumları ve itibar puanını görmek istemesi beklenen bir durumdur. ***A***, ***S***'den bir satın alma işlemi gerçekleştirdikten sonra ***A***'nın ***S*** hakkında geri bildirim vermesine ve ***S***'yi puanlamasına izin verilir. ***A***'nın ***S*** hakkında geri bildirim verebilmesi için, ***S*** veya pazar yeri ***P*** tarafından üretilen bir geri bildirim jetonu almış olması gerekir. ***A***'nın geri bildirim vermesi bir satın alma işlemi gerçekleştirmesine bağlı olsa da ***A***'nın kimliği ile verdiği geri bildirim arasında bir bağlantı kurulamaz.

Satıcı: Satıcı ***S***, e-ticaret işlemlerinde çevrim içi olarak mal veya hizmet sunan varlıktır. ***S***'nin çevrim içi bir pazar yeri olan ***P***'de bir dükkânı olabilir veya kendi çevrim içi satış platformuna sahip olabilir. Bir satın alma işlemi gerçekleştikten sonra ***S*** veya ***P***, ***A*** için bir geri bildirim jetonu üretir. ***A*** bu geri bildirim jetonunu kullanarak daha sonra ***S*** için geri bildirim gönderebilir.

Pazar yeri: Pazar yeri ***P***, satıcılar için çevrim içi dükkânlar sağlayarak alıcıların satıcılardan satın alacakları mal ve hizmetleri bulmaları için çevrim içi bir platform sağlar. Genellikle bir ***P*** alıcılardan geri bildirim toplamak, saklamak ve sunmak için dahili bir geri bildirim sistemine sahiptir. Bununla birlikte, modelimiz geri bildirim sistemini ***P***'nin dışında tutarak ***P***'den bağımsız hale getirir.

Yasal Merci: Modelimizde yer alan yasal merci ***YM***, mevzuatla yetkilendirilmiş şirketlerin süreç ve kayıtlarından sorumlu kuruluşlardır. Bu nedenle ***YM***, ***S***'ye dijital kimlik vermek

için tek yetkili varlıktır. ***YM*** tarafından ***S***'ye verilen dijital kimlikler, ***S***'nin sisteme biricik kimlikle kayıt olmasını garanti altına alır.

İtibar sistemimiz iki alt sistemden oluşmaktadır:

1. Doğrulanabilir Kimlik Alt Sistemi
2. Geri Bildirim Toplama Alt Sistemi

5.2.1. Doğrulanabilir kimlik alt sistemi

Doğrulanabilir Kimlik Alt Sistemi ***DKS***, doğrulanabilir kimliklerin sağlayıcılar tarafından verilmesini ve kimliklerin geçerliliğinin doğrulanmasını sağlar. İtibar sistemimiz kapsamında üç farklı doğrulanabilir kimlik bulunmaktadır:

- Yasal merciler tarafından satıcılara verilen dijital kimlikler,
- Alıcılara satıcılar veya pazar yerleri tarafından satın alma işlemi gerçekleştikten sonra verilen geri bildirim jetonları,
- Geri bildirim veren alıcılara Geri Bildirim Toplama Sistemi tarafından verilen indirim jetonları.

Doğrulanabilir Kimlik Alt Sistemi Hyperledger Indy blok zinciri ile birlikte Hyperledger Aries ve Ursa kütüphaneleri kullanılarak geliştirilmiştir. DKS'nin ilk kurulumunda sistemde üç temel şema bulunması gerekmektedir.

1. Satıcı Dijital Kimliği Şeması
2. Geri Bildirim Jetonu Şeması
3. İndirim Jetonu Şeması

Satıcı dijital kimliği şeması, dijital kimlik güven çerçevesinde tanımlandığı şekilde en az aşağıdaki bilgileri içermelidir.

```
{
   "@context": [
      "https://www.w3.org/2018/credentials/v1",
      "https://www.ticaret.gov.tr/digital-identity/schemas/v1",
```

```
        "https://w3id.org/security/suites/ed25519-2020/v1"
          ],
    "type": ["VerifiableCredential", "TemelKimlik"],
    "issuer": "...",
    "issuanceDate": "...",
    "expirationDate": "...",
    "credentialSubject": {
          "id": "..."
          "kimlik": {
                    "turu": " TemelKimlik",
                    "unvan": "...",
                    "vergiKimlikNo": "..."
                    "vergiDairesi": "...",
                    "kurulusTarihi": "...",
                    "adres": "...",
                    "sehir": "..."
                  }
    },
    "proof": {
          "type": "Ed25519Signature2020",
          "created": "…",
          "verificationMethod”: “…”,
          "proofPurpose": "…",
          "proofValue": "…",
    }
}
```


Geri bildirim jetonu, satıcı veya pazar yeri bilgisi ile birlikte, gerçekleşen satın alma işleminin tutarını da içermelidir.


```
{
   "@context": [
      "https://www.w3.org/2018/credentials/v1",
      "https://www.ticaret.gov.tr/digital-identity/schemas/v1",
      "https://w3id.org/security/suites/ed25519-2020/v1"
        ],
    "type": ["VerifiableCredential", "GeriBildirimJetonu"],
    "issuer": "...",
    "issuanceDate": "...",
    "expirationDate": "...",
```

```
    "credentialSubject": {
          "id": "..."
          "jeton": {
                    "turu": " GeriBildirimJetonu ",
                    "satıcıVergiKimlikNo": "...",
                    "pazaryeriVergiKimlikNo": "...",
                    "islemTutari": "..."
                }
    },
    "proof": {
          "type": "Ed25519Signature2020",
          "created": "…",
          "verificationMethod”: “…”,
          "proofPurpose": "…",
          "proofValue": "…",
    }
}
```


İndirim jetonu ise satıcı veya pazar yeri bilgisi ile birlikte, gerçekleşen satın alma işleminin tarihini, tutarını ve indirim tutarını içermelidir.


```
{
   "@context": [
      "https://www.w3.org/2018/credentials/v1",
      "https://www.ticaret.gov.tr/digital-identity/schemas/v1",
      "https://w3id.org/security/suites/ed25519-2020/v1"
       ],
    "type": ["VerifiableCredential", "IndirimJetonu"],
    "issuer": "...",
    "issuanceDate": "...",
    "expirationDate": "...",
    "credentialSubject": {
          "id": "..."
          "jeton": {
                    "turu": " IndirimJetonu",
                    "satıcıVergiKimlikNo": "...",
                    "pazaryeriVergiKimlikNo": "...",
                    "islemTarihi": " IndirimJetonu",
                    "islemTutari": "...",
                    "indirimTutari": "..."
```

```
                    }
    },
    "proof": {
        "type": "Ed25519Signature2020",
        "created": "…",
        "verificationMethod”: “…”,
        "proofPurpose": "…",
        "proofValue": "…",
    }
}
```

Yukarıdaki şemalarda tanımlanan alanların doğrulanabilir kimliklerde yer alması, bu alanların her zaman doğrulanabilir kimliğin kanıtını sunarken açığa çıkarılmasını ve karşı taraf tarafından bilinmesini zorunlu kılmamaktadır. Örneğin S veya P, alıcıyı bir kampanyadan faydalandırmaya karar vermek için indirim jetonundaki işlem tutarının belli bir tutarın üzerinde olup olmadığını bilmek isteyebilir. İşlem tutarının belli bir tutarın üzerinde olup olmadığını ispatlamak için indirim jetonundaki **islemTutari** alanının açığa çıkarılması gerekmemektedir. Bunun yerine sıfır bilgi ispatının sağladığı kriptografik kanıt mekanizması sayesinde ***A***, işlem tutarının belli bir değerden büyük olduğunu ***S*** veya ***P***'ye ispatlayabilmektedir.

5.2.2. Geri bildirim toplama alt sistemi

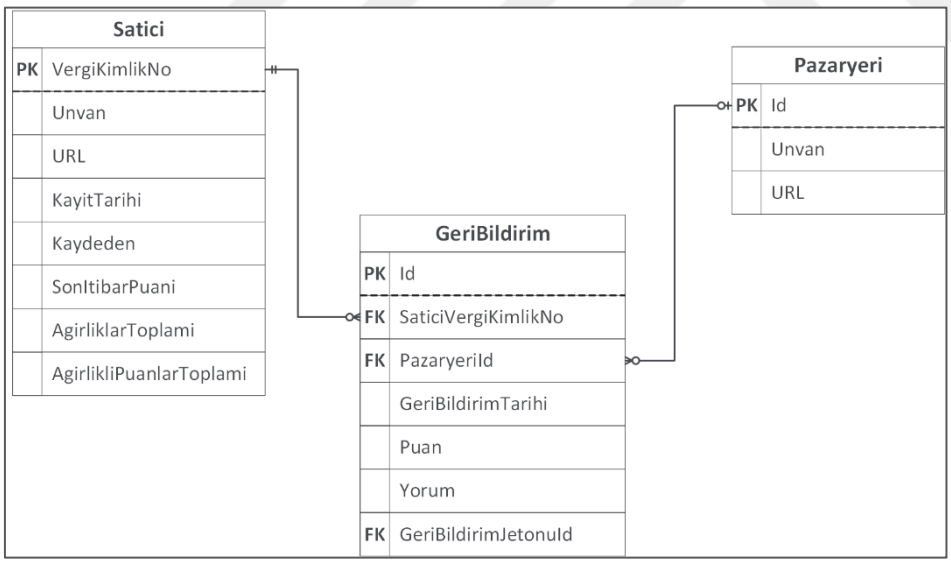
Geri Bildirim Toplama Alt Sistemi ***GTS*** alıcılardan geri bildirimleri ve puanlamaları toplayarak satıcıların itibar puanını hesaplar. Bir alıcının bu alt sisteme geri bildirim gönderebilmesi için, tamamlanmış bir e-ticaret işleminin kanıtı olarak geri bildirim jetonunu sağlaması gerekir. Alt sistem, geri bildirim jetonunu geçerlilik, son kullanma tarihi, tek seferlik kullanım ve satıcı eşleştirme kısıtlamaları açısından doğrular. Geri bildirim jetonu tüm doğrulamaları geçerse, alt sistem blok zincirine geri bildirimi kaydeder ve satıcı için nihai itibar puanını hesaplar.

Alt sistem geri bildirimi kaydettikten sonra geri bildirimi sağlayan alıcıya geri bildirimin kanıtı olarak indirim jetonu verir. İndirim jetonu, alıcıları geri bildirim göndermeye teşvik eden bir mekanizmadır. Sistemdeki e-ticaret platformları, özel kampanyalar, indirim kuponları veya başka teşvik yöntemleri sağlamak için bu indirim jetonlarını kabul edebilir.

Bu alt sistem Hyperledger Fabric blok zinciri alt yapısı kullanılarak geliştirilmiştir. Gerekli işlevler ise Hyperledger Fabric alt yapısında zincir kodu (chaincode) olarak adlandırılan akıllı kontratlar ile geliştirilmiştir.

Bu alt sistem, satıcı dijital kimlikleri ve geri bildirim jetonları için Doğrulanabilir Kimlik ekosisteminde Kimlik Talep Eden görevi görür. Satıcılar tarafından sunulan dijital kimlikleri ve alıcılar tarafından sunulan geri bildirim jetonlarını doğrular ve saklar. Alt sistem ayrıca indirim jetonları için Doğrulanabilir Kimlik ekosisteminde kimlik sağlayıcı (Issuer) olarak görev yapar. İndirim jetonları, geri bildirim sağlayan alıcılara özel teklifler veya kampanyalar sunmak için pazar yerleri veya satıcılar tarafından doğrulanır.

GTS kriptografik olarak imzalanmış doğrulanabilir kimlikleri saklamanın yanı sıra akıllı kontrat işlevlerini desteklemek amacıyla başka bağlantılı tablolar da bulundurur. ***GTS***'nin Hyperledger Fabric kayıt defteri durum veri tabanında saklanan veriler için mantıksal veri modeli aşağıdaki şekilde gösterilmiştir.



Şekil 5.1. GTS mantıksal veri modeli

Mantıksal veri modelinde görüldüğü gibi, geri bildirim sağlayan alıcılarla geri bildirimler arasında bağlantı sağlayacak herhangi bir bilgi veri tabanında saklanmamaktadır. Geri bildirimi sağlayan alıcı tarafından gönderilen geri bildirim jetonunun tanımlayıcısı GeriBildirim tablosunda GeriBildirimJetonuId alanında saklanmaktadır. Bu tanımlayıcı geri bildirim jetonu üretilirken geri bildirimi sağlayan alıcı tarafından oluşturulduğundan geri bildirim jetonunu veren satıcı veya pazar yeri tarafından bilinmemektedir. Bu nedenle

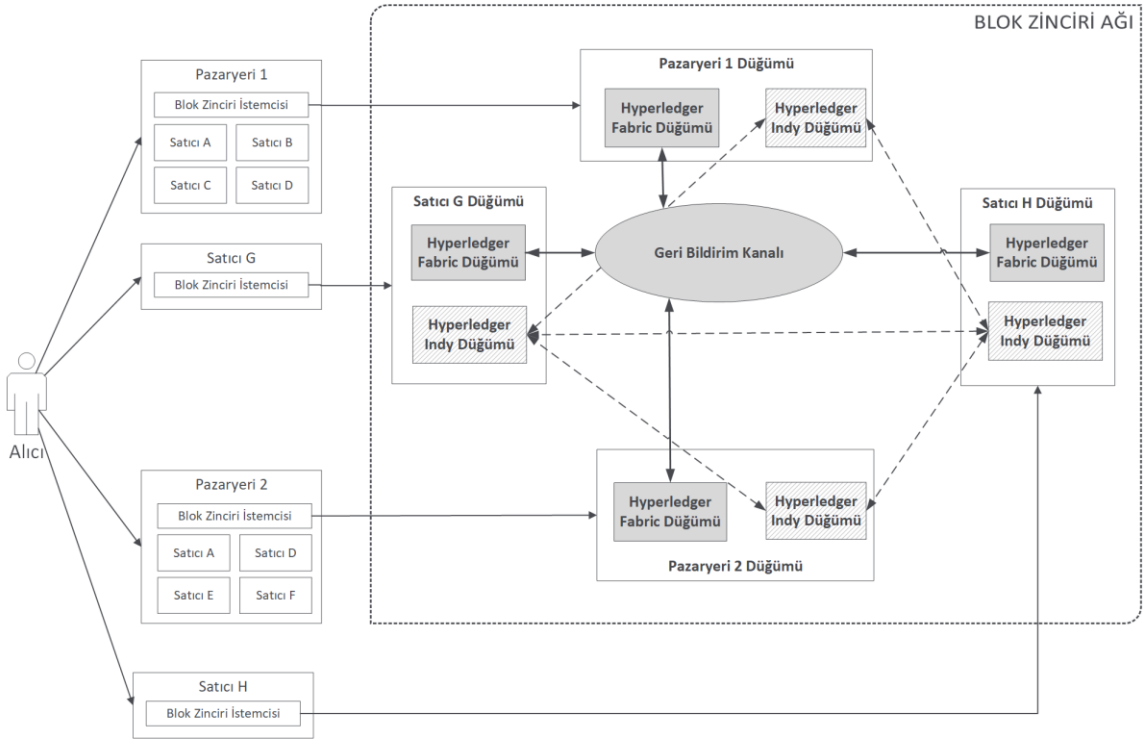
GeriBildirimJetonuId ile geri bildirimi sağlayan alıcıyı ilişkilendirecek bir bilgi bulunmamaktadır. GeriBildirimJetonuId değerini saklamanın amacı ise, aynı geri bildirim jetonu ile birden fazla geri bildirim gönderilmesini engellemektir. Böylelikle bir satın alma işlemi için en fazla bir geri bildirimde bulunulabilmektedir. Bu veri modeli ayrıca satıcıların da sisteme SaticiVergiKimlikNo değeri ile biricik olarak kayıt yapmalarını sağlamaktadır.

GTS kapsamında aşağıdaki akıllı kontratlar Hyperledger Fabric üzerinde geliştirilmiştir:

- **saticiKaydet**: İtibar sisteminin müstakbel bir satıcısı olan ***S***, saticiKaydet akıllı kontratı yöntemini çağırır ve kayıt için ***YM***'den aldığı dijital kimliğini sağlar. Alt sistem, Hyperledger Indy blok zinciri aracılığıyla, sunulan dijital kimliğin geçerli olduğunu doğrular. Dijital kimlik geçerliyse, alt sistem sunulan dijital kimlikten bilgi alır ve blok zincirinde satıcı kaydı oluşturur veya günceller.
- **itibarPuaniGetir**: Tüm kullanıcılar itibarPuaniGetir akıllı kontrat yöntemini çağırarak bir satıcının itibar puanını görebilir. Bu yöntem, hesaplanan son itibar puanını döndürür.
- **tumGeriBildirimleriGetir**: Tüm kullanıcılar, tumGeriBildirimleriGetir akıllı kontrat yöntemini çağırarak, bir satıcıyla ilgili belli bir tarih aralığındaki tüm geri bildirimlerin listesini alabilir. Bu yöntem, geri bildirim puanı ve yorum dahil olmak üzere tüm geri bildirimlerin listesini döndürür.
- **geriBildirimGonder**: Bir alıcı, geriBildirimGonder akıllı kontrat yöntemini çağırarak sisteme yeni bir geri bildirim gönderir. Alıcı geri bildirim gönderebilmek için bir satıcıdan veya bir pazar yerinden geri bildirim jetonu almış olmalı ve bu jetonu tamamlanan e-ticaret işleminin kanıtı olarak sunmalıdır. Alt sistem, Hyperledger Indy blok zinciri aracılığıyla, sunulan geri bildirim jetonunun imzalarının geçerli olduğunu ve geri bildirim jetonunun süresinin henüz dolmadığını doğrular. Bu doğrulamalardan geçtikten sonra alt sistem satıcının sistemde kayıtlı olduğunu ve sunulan geri bildirim jetonunun daha önce kullanılmadığını kontrol eder. Tüm kontroller tamamlandıktan sonra, geri bildirim tarihi, puan ve yorum ayrıntılarını içeren geri bildirim kaydı blok zincirine eklenir. Satıcının itibar puanı hesaplanır ve veri tabanında güncellenir. Geri bildirimi kaydettikten sonra, alt sistem geri bildirimi sağlayan alıcıya geri bildirim gönderiminin kanıtı olarak indirim jetonu verir.

Alıcılar özel teklif ve kampanyalardan faydalanmak üzere indirim jetonlarını satıcılara ve pazar yerlerine sunarken sıfır bilgi ispatı mekanizmaları da uygulanabilir. Bir pazar yeri veya satıcı, alıcıyı özel teklif veya kampanyadan faydalandırmak için indirim jetonuna ait satın alma işleminin o platformdan yapıldığını doğrulamak isteyebilir. Bu durumda alıcı, indirim jetonuna ait satın alma işleminin hangi pazar yeri veya satıcıdan yapıldığını doğrudan açıklamadan bu şartın sağlanıp sağlanmadığını ispatlayabilir.

DKS ve ***GTS*** alt sistemlerinin oluşturduğu genel sistem ağ mimarisi aşağıdaki şekilde gösterilmiştir.



Şekil 5.2. Genel sistem ağ mimarisi

Şekilde görüldüğü üzere, itibar sisteminin katılımcıları, blok zinciri düğümlerini sağlayarak blok zinciri ağını oluşturur. Her katılımcı iki düğümden oluşur: bir düğüm Hyperledger Fabric blok zinciri için ve diğer düğüm Hyperledger Indy blok zinciri içindir. Bu iki blok zincirin entegrasyonu akıllı sözleşmeler ile yapılır. Alıcılar, pazar yerlerinin ve satıcıların e-ticaret platformları aracılığıyla blok zinciri ile etkileşime girer. Alıcıların blok zinciri etkileşimi için bağımsız bir platform da bulunabilir.

5.3. Süreçler

Tüm e-ticaret sürecini aşağıdaki dört alt süreç ile tanımlamak mümkündür.

1. Satıcı Kayıt Fazı
2. Alışveriş Fazı
3. Hizmet Sunumu Fazı
4. Geri Bildirim Fazı

5.3.1. Satıcı kayıt fazı

Satıcı kayıt fazının ilk aşaması ***YM*** tarafından ***S***'ye dijital kimlik verilmesi aşamasıdır.

Algoritma 1: Dijital Kimlik Verme

Ön Şart: ***YM*** ve ***S*** arasında bağlantı oluşturuldu.

1. ***S***, ***YM***'ye kimlik talebini gönderir.
2. **EĞER** ***YM*** kayıtlarında ***S***'ye ait geçerli bir kayıt varsa
3. ***YM***, ***S*** için dijital kimlik üreterek ***S***'ye gönderir
4. ***S*** dijital kimliği elektronik cüzdanında saklar
5. **EĞER** ***YM*** kayıtlarında ***S***'ye ait geçerli bir kayıt yoksa
6. ***YM***, ***S***'nin dijital kimlik talebini reddeder
7. **SON**

S'nin dijital kimliğini aldıktan sonra ***GTS***'ye kayıt talebinde bulunması ve ***GTS*** tarafından geçerli dijital kimliğinin olduğu doğrulandıktan sonra ***GTS*** blok zincirine eklenmesi ise satıcı kayıt fazının ikinci aşamasını oluşturur.

Algoritma 2: Satıcının ***GTS***'ye Eklenmesi

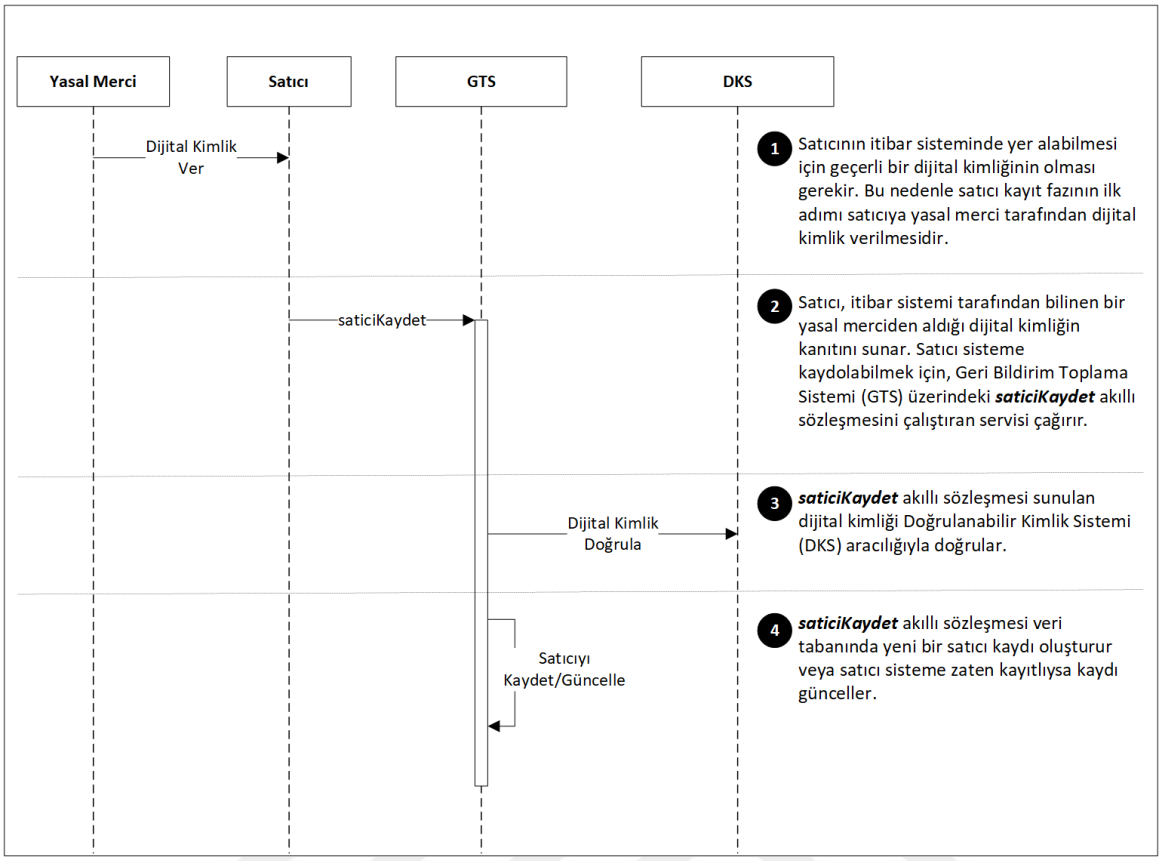
Ön Şart: ***S*** geçerli bir dijital kimliğe sahip.

1. ***S***, ***GTS***'ye kayıt olmak için talebini gönderir
2. ***GTS***, ***S***'nin daha önceden bilinen bir YM'den aldığı bir dijital kimlik için kanıt

gönderip göndermediğini kontrol eder

3. **EĞER** kanıt bulunamadıysa
4. ***GTS***, ***S***'den kanıt sunmasını ister
5. ***S*** daha önceden aldığı dijital kimliğe ilişkin kanıtı üreterek ***GTS***'ye gönderir
6. ***GTS*** kanıtın doğruluğunu ve geçerliliğini ***DKS*** blok zinciri aracılığıyla kontrol eder
7. **EĞER** kanıt geçerliyse
8. ***GTS*** dijital kimlik kanıtını elektronik cüzdanında saklar
9. **EĞER** kanıt geçerli değilse
10. ***GTS*** satıcının sisteme kaydını reddeder ve hata döner
11. ***GTS*** *saticiKaydet* akıllı kontrat metodunu çağırır.
12. *saticiKaydet* akıllı kontrat metodu ***S***'ye ilişkin kaydı ***GTS*** blok zincirine yazar
13. **SON**

Aşağıdaki sıralama diyagramı satıcının sisteme kaydedilmesi ile ilgili işlemleri göstermektedir.



Şekil 5.3. Satıcı kaydı sıralama diyagramı

5.3.2. Alışveriş fazı

Alışveriş fazında alıcı, *itibarPuaniGetir* ve *tumGeriBildirimleriGetir* akıllı kontrat metotlarını çağırarak bir satıcının genel itibar puanını ve tüm geri bildirimlerini görmek isteyebilir. Akıllı kontrat metotlarının çağrılması, satıcı, pazar yeri veya başka bir platform aracılığıyla gerçekleştirilebilir. Alıcı, geri bildirimlere ve itibar puanına göre satıcının güvenilir olup olmadığına karar verebilir.

Alıcı, satıcıyla alışverişe devam etmeye karar verirse, bir sonraki adım ödemeyi yapmak ve hizmetin satıcı tarafından teslim edilmesini beklemektir. Alıcı ödemeyi tamamladıktan sonra, satıcı veya pazar yeri alışveriş işleminin kanıtı olarak geri bildirim jetonu üreterek alıcıya verir. Alıcı, geri bildirim jetonunu bir süre elinde tutabilir ve jetonun geçerli olduğu süre boyunca daha sonra geri bildirim göndermeyi tercih edebilir.

Algoritma 3: Geri Bildirim Jetonu Verme

Ön Şart: ***A*** ve ***S*** arasında bağlantı oluşturuldu. ***A***, ***S*** üzerinden bir satın alma işlemi

gerçekleştirdi.

1. **EĞER** İşlem Tutarı >= Alt Sınır
2. ***S***, ***A*** için geri bildirim jetonu üreterek ***A***'ya gönderir
3. ***A*** geri bildirim jetonunu elektronik cüzdanında saklar
4. **EĞER** İşlem Tutarı < Alt Sınır
5. ***S*** geri bildirim jetonu üretmez.
6. **SON**

5.3.3. Hizmet sunumu fazı

Hizmet sunumu fazının nasıl gerçekleşeceği, satıcının sunduğu hizmetin türüne göre değişmektedir. Satıcının fiziksel mal satışı yaptığı durumlarda, malın alıcıya ulaşması ödemeden sonra günler ve hatta haftalar alabilmektedir. Hizmet sunumu fazı, satıcının alıcıya talep ettiği mal veya hizmeti sağladığı ve sistemin dışında gerçekleşen bir fazdır. Bu nedenle bu fazda sistem üzerinde herhangi bir işlem gerçekleşmez.

5.3.4. Geri bildirim fazı

Alıcı, satıcıdan veya pazar yerinden geri bildirim jetonunu aldıktan sonra ve geri bildirim jetonunun süresi dolmadan önce istediği zaman satıcı için geri bildirim gönderebilir. Geri bildirimin hizmet sunumu aşamasından sonra verilmesi yaygın bir uygulama olsa da sistemde katı bir kısıtlama değildir. Ayrıca, hizmet sunumu asla gerçekleşmeyebilir ve bu durumda alıcı muhtemelen satıcı için olumsuz geri bildirim göndermeye daha istekli olacaktır.

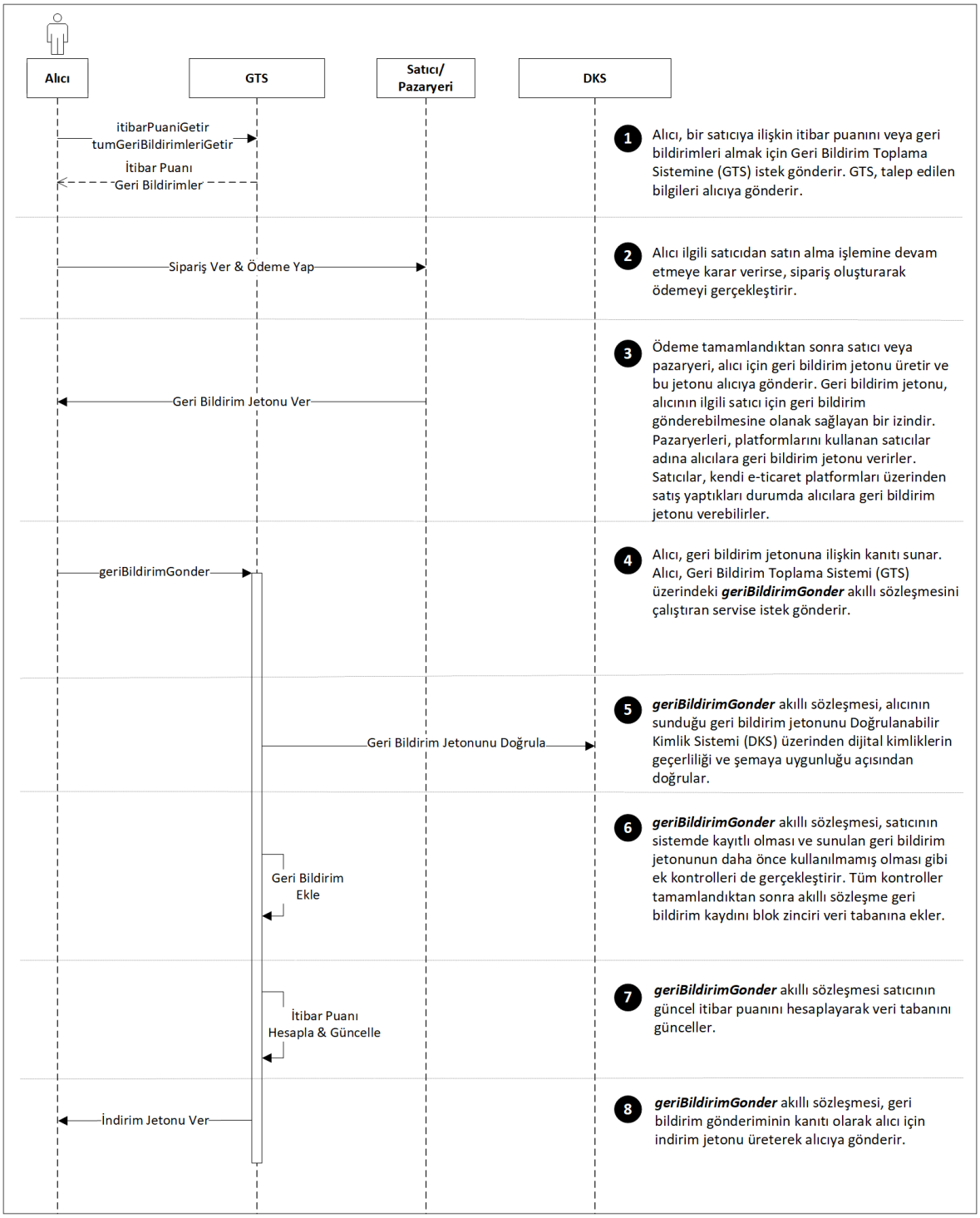
Algoritma 4: Geri Bildirim Gönderilmesi

Ön Şart: ***A***, ***S***'den geri bildirim jetonu aldı.

1. ***A***, ***GTS***'ye ***S*** için geri bildirim gönderir
2. ***GTS***, ***A***'nin ***S***'den alışveriş yaptığına dair kanıt göndermesini talep eder
3. ***A***, ***S***'den aldığı geri bildirim jetonuna ilişkin kanıt üreterek ***GTS***'ye gönderir
4. ***GTS*** kanıtın doğruluğunu ve geçerliliğini ***DKS*** blok zinciri aracılığıyla kontrol eder
5. **EĞER** kanıt geçerliyse

6. ***GTS***, aynı geri bildirim jetonunun daha önce başka geri bildirim için kullanılıp kullanılmadığını kontrol eder
7. **EĞER** geri bildirim jetonu daha önce kullanılmadıysa
8. ***GTS*** geri bildirim jetonu kanıtını elektronik cüzdanında saklar
9. ***GTS*** geri bildirimi blok zincirine yazar
10. ***GTS S***'nin itibar puanını tekrar hesaplar ve blok zincirinde günceller
11. ***GTS A***'ya indirim jetonu gönderir
12. ***A*** indirim jetonunu elektronik cüzdanında saklar
13. **EĞER** geri bildirim jetonu daha önce kullanıldıysa
14. ***GTS*** geri bildirimi reddeder ve hata döner
15. **EĞER** kanıt geçerli değilse
16. ***GTS*** geri bildirimi reddeder ve hata döner
17. **SON**

Aşağıdaki sıralama diyagramı alışveriş ve geri bildirim fazlarına ilişkin işlemleri göstermektedir. Hizmet sunumu fazında sistemde herhangi bir işlem gerçekleşmediğinden hizmet sunumu fazı sıralama diyagramında gösterilmemiştir.



Şekil 5.4. Hizmet sunumu fazı sıralama diyagramı

5.4. İtibar Puanı ve İndirim Jetonu Tutarı Hesaplama

S için itibar puanının hesaplanmasındaki ana girdi, ***A***'nın geri bildirimin bir parçası olarak sağladığı satıcı puanıdır. Sistemde herhangi bir ***S*** için itibar puanı aşağıdaki parametreleri

kullanan bir formülle alıcıların verdiği puanların ağırlıklı ortalaması olarak hesaplanmaktadır.

Satın Alma İşleminin Üzerinden Geçen Zaman

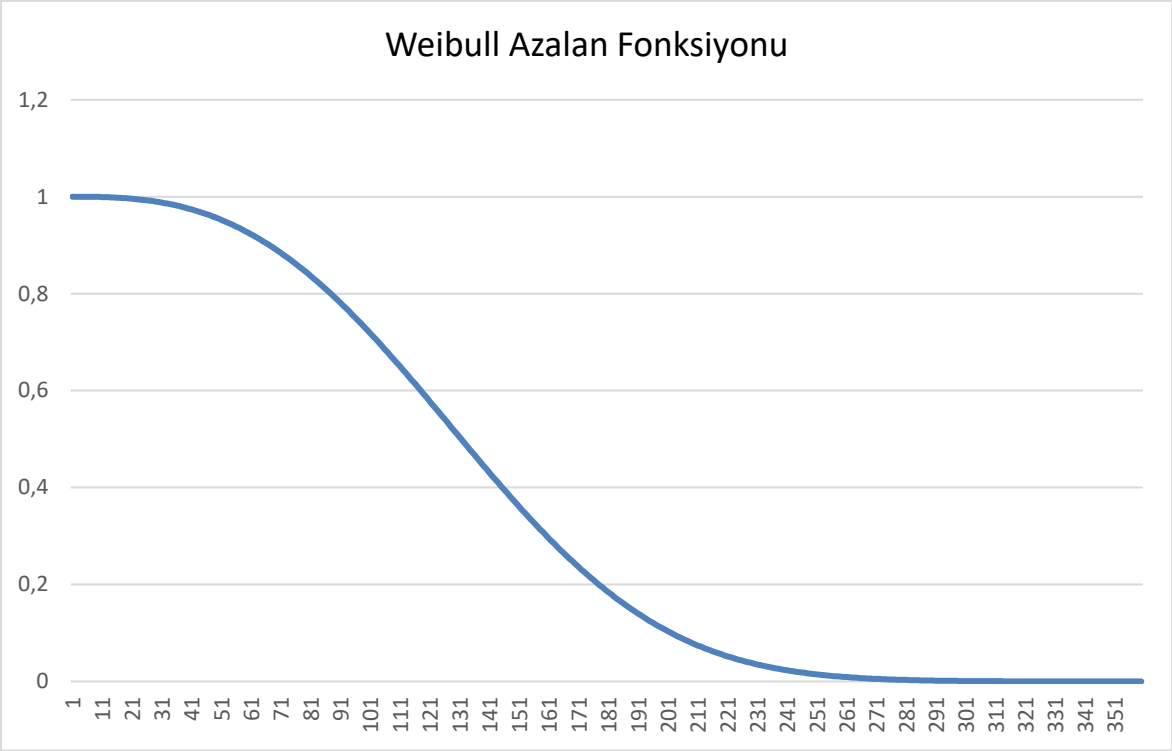
Satın alma işleminin üzerinden geçen zamanın ağırlık etkisi, geri bildirimlerin öneminin zaman geçtikçe nasıl azaldığı ile orantılı olmalıdır. Geri bildirimlerin zamana göre önemini belirlemek için Jøsang, Ismail ve Boyd'un (2006) araştırmasında yer alan internet üzerindeki en büyük açık artırma usulü alışveriş sitesi olan eBay'in geri bildirimleri hangi zaman aralıkları ile gösterdiği bilgisi kullanılmıştır. Bu bilgiye göre eBay'de geri bildirimler son 7 gün, son 30 gün ve son altı aylık zaman pencerelerinde gösterilmektedir. Buna göre geri bildirimlerin zamana göre etkisi için aşağıdaki kriterler belirlenmiştir.

- İlk 7 gün içinde verilen geri bildirimlerin etkisi 0,99'un altına düşmemeli,
- İlk 30 gün içinde verilen geri bildirimlerin etkisi 0,95'in altına düşmemeli,
- 6 aylık süre sonunda geri bildirimlerin etkisi 0,05'in altına düşmeli

Verilen kriterlere göre satın alma işleminin üzerinden geçen zamanın itibar puanına etkisi, zamana göre giderek azalan fakat azalma oranının sabit olmadığı bir azalma fonksiyonu ile hesaplanabilir. Bunun için en uygun değişken oranlı azalan fonksiyonu Weibull azalan fonksiyonu olarak belirlenmiştir. Weibull azalan fonksiyonu genellikle arızaya kadar geçen süre verilerini modellemek için kullanılır. Fakat sabit bir azalma oranı olmayan azalan fonksiyonlarını modellemek için de uygulanabilir. Başlangıç değeri 1 olan bir Weibull fonksiyonunun formülü aşağıdaki şekilde basitleştirilebilir.

$$P(t) = e^{-(\frac{t}{\lambda})^k} \tag{5.1}$$

Bu formülde *P(t),* fonksiyonun *t* gün sonraki değerini, λ ölçek parametresini, *k* ise şekil parametresini göstermektedir. Weibull fonksiyonunun yukarıda verilen kriterlerdeki süreye göre etki değerlerine ulaşmak için λ ve *k* değerleri sırasıyla 150 ve 2,8 olarak bulunur. Bu değerlerle birlikte fonksiyonun grafiği aşağıdaki gibi ortaya çıkmaktadır.



İşlem tutarı

İtibar puanı hesaplaması işlem tutarını dikkate almazsa ve tüm işlem tutarları için puanlamanın ağırlığı aynı olursa, itibar sistemi kötüleme saldırılarına açık hale gelmektedir. Bu tür saldırılarda saldırganlar çok sayıda düşük fiyatlı işlem gerçekleştirerek aynı satıcı için çok sayıda düşük puan gönderebilmektedir. Geri bildirim puanının itibar puanı hesaplamadaki ağırlığının işlem tutarına bağlı hale getirilmesi, bu şekilde yapılan kötüleme saldırılarının en aza indirilmesini sağlar. İşlem tutarının ağırlık etkisi aşağıdaki formülle hesaplanır.

$$\beta(A) = \begin{cases} 1 & A > \alpha \\ 0 & A < \mu \\ A_{normalize} & diğer\ durumlar \end{cases} \tag{5.2}$$

Bu formülde β işlem tutarının ağırlık etkisi değerini, A işlem tutarını, α işlem tutarının ağırlığının 1 olacağı sınır değerini ve μ işlem tutarının ağırlığının 0 olacağı sınır değerini ifade etmektedir. İşlem tutarının ağırlık etkisi, tutar α sınır değerinin altına indikçe azalır ve μ sınır değerine ulaştığında sıfırlanmış olur. α sınır değerinin üstündeki tutarlar için ağırlık etkisi 1, μ sınır değerinin altındaki tutarlar için ağırlık etkisi 0 olarak alınır.

$A_{normalize}$ değeri, $[\mu - \alpha]$ aralığındaki işlem tutarının [0-1] aralığındaki bir değere normalize edilmesi ile elde edilir. Bu değer aşağıdaki formülle hesaplanır.

$$A_{normalize} = \frac{A - \mu}{\alpha - \mu} \tag{5.3}$$

Her bir geri bildirim puanı için ağırlık değeri w aşağıdaki formülle hesaplanır.

$$w = P(t) \times \beta(A) \tag{5.4}$$

$\boldsymbol{S}$'nin itibar puanı, geri bildirim puanlarının ağırlıklı ortalaması olarak aşağıdaki formülle hesaplanır.

$$R_s = \frac{\sum_{i=1}^{n} \omega_i \times \chi_i}{\sum_{i=1}^{n} \omega_i} \tag{5.5}$$

Bu formülde w_i değeri, her bir geri bildirim puanının ağırlığını, x_i değeri geri bildirim puanını ve n değeri $\boldsymbol{S}$ için verilen toplam geri bildirim sayısını ifade etmektedir.

İtibar sistemimiz bir satıcının itibar puanını her defasında tüm geri bildirim puanlarını kullanarak hesaplamak yerine daha verimli bir yöntem kullanmaktadır. Yeni bir geri bildirim puanı geldiğinde itibar puanını tekrar hesaplamak için sistemde tüm ağırlıkların toplamı olan W_t değeri ile tüm ağırlıklandırılmış geri bildirim puanlarının toplamı olan X_t değeri de saklanır. Yeni gelen geri bildirim puanı ile birlikte yeni itibar puanı aşağıdaki formülle hesaplanır.

$$R_s = \frac{X_t + \omega \times x}{W_t + \omega} \tag{5.6}$$

Bu formülde x değeri yeni alınan geri bildirim puanını ve w ise yeni geri bildirim puanı için hesaplanan ağırlık değerini ifade eder.

İndirim jetonu, satıcı ***S*** veya pazar yeri ***P*** tarafından alıcı ***A***'ya geri bildirim göndermesi için bir teşvik mekanizması olarak verilir. İndirim jetonundaki indirim tutarının sabit bir oran veya tutar olmaması ve itibar puanı hesaplamasında kullanılan aynı parametrelere bağlı olarak hesaplanması gerekir. Bu nedenle, indirim tutarının hesaplanması da w ağırlık değerini içerir.

İndirim tutarının hesaplanması için w değerinin yanı sıra her satıcı için ayarlanabilecek bir indirim oranı r belirlenmesi gerekir. r değerinin her satıcı için ayrı belirlenebilmesi, satıcıların geri bildirim sonrası ne kadarlık bir indirim jetonu sağlayacaklarını kendilerinin belirlemesini sağlar. İndirim jetonunda yer alan indirim tutarı aşağıdaki formülle hesaplanır.

$$D = A \times w \times r \tag{5.7}$$

Bu formülde D indirim tutarını, A işlem tutarını, w itibar puanı hesaplamasında kullanılan ve her bir geri bildirim için hesaplanan ağırlık değerini ve r her satıcı için değişken olan indirim oranını ifade eder.

5.5. Modelin Güvenliği

Bu bölümde modelimizin güvenlik yönüyle hangi özellikleri içerdiği ve güvenlik analizi yer almaktadır.

5.5.1. Mahremiyetin korunması

Bu tez çalışması kapsamında önerdiğimiz model alıcıların gizliliğini korumak için sıfır bilgi ispatı algoritmalarını kullanır. Hyperledger Indy tarafından sağlanan sıfır bilgi ispatı algoritmaları, IBM tarafından geliştirilen Identity Mixer (idemix) kriptografi kütüphanesi ile aynı şifreleme ilkelerine dayanmaktadır. Idemix, birden fazla mesajın imzalanmasını ve imza sahipliğine ilişkin verimli sıfır bilgi kanıtlarını destekleyen kör bir imza şemasından oluşturulmuştur. Temel olarak idemix'te kullanılan dijital imza şeması, dijital kimlik vermek için kullanılan Camenisch-Lysyanskaya (CL) imza şemasıdır (Camenisch ve Lysyanskaya, 2003). CL imza şeması, bir kullanıcının sıfır bilgi ispatı kullanarak temel kimlik bilgilerini ifşa etmeden bir imzası olduğunu kanıtlamasına olanak tanır. Bir kullanıcı, bir kimlik

sağlayıcısının kendisine bir kimlik verdiğini kanıtlayabilir. Ayrıca, kimlik bilgisi için sağlayıcının imzasını bildiğini gösteren bir sıfır bilgi ispatı kullanarak kimlik bilgisinin özniteliklerinin bazılarını veya tümünü gizleyebilir veya açığa çıkarabilir. CL imza şemasının diğer bir özelliği, m_1, m_2, …, m_L şeklinde L adet mesajın imzalanmasını desteklemesidir. Çoklu mesaj imzalama özelliği, tez çalışmamızdaki kullanımı kapsamında bir dijital kimlikte bulunan birden fazla özniteliğin imzalanmasına karşılık gelmektedir. CL imza şeması aşağıdaki algoritmaları içerir (Camenisch, 2010).

GenerateKey$(l_n) \rightarrow (P_k, S_k)$: l_n girdisi üzerine (P_k, S_k) adında bir genel-özel anahtar çifti çıktısı üretir. Burada l_n, RSA modülü n'nin uzunluğunu gösterir.

Mesaj Uzayı: l_m bir parametre olsun. Mesaj uzayı, şu küme olarak tanımlanır: $\{(m_0, m_1, ..., m_{L-1}): m_i \in \pm \{0,1\}^{lm}\}$. Mesaj uzayı, şifreleme algoritması tarafından işlenebilecek ve iletilmesi amaçlanan mesajların yer aldığı kümedir. Bu ifadede L dizideki eleman sayısını gösterir.

Sign$((m_0, m_1, ..., m_{L-1}), S_k) \rightarrow \delta$: $(m_0, m_1, ..., m_{L-1})$ girdisi üzerine özel anahtar S_k ile bir dijital imza δ çıktısı üretir.

Verify$((m_0,m_1,...,m_{L-1}),\delta,P_k) \rightarrow$ ***success/fail***: $(m_0, m_1, ..., m_{L-1})$ mesajı, δ imzası ve P_k genel anahtarını girdi olarak alan algoritma, δ'nin $(m_0, m_1, ..., m_{L-1})$ üzerindeki geçerliliğini doğrular. Eğer geçerliyse, algoritma başarı (success) çıktısı verir. Aksi halde, başarısızlık (fail) çıktısı verir.

Kimlik verme, kimlik bilgisine ilişkin kanıt sunma ve kanıtın doğrulanması aşamalarını açıklayan protokol şu şekilde özetlenebilir (Lodder ve Khovratovich, t.y.):

1. Kimlik sağlayıcı, bir kimlik bilgisi şeması $\boldsymbol{S}$ belirler. Kimlik bilgisi şeması tanımı, bir kimlik bilgisindeki öznitelik sayısı l, gizli özniteliklerin indeksleri $A_h \subset \{1, 2, ..., l\}$, iptal edilemeyen kimlik bilgisi özniteliği sayısı l_r, kriptografik imza türü, genel anahtar P_k ve iptal edilmeme genel anahtar P_r'yi içerir. Kimlik sağlayıcı, kimlik bilgisi tanımını blok zincirinde yayınlar.
2. Kimlik sahibi, blok zincirinden kimlik bilgisi şemasını alır ve gizli öznitelikleri belirler.
3. Kimlik sahibi, kimlik sağlayıcıdan bir kimlik bilgisi talep eder.

4. Kimlik sağlayıcı, özniteliklerin, iptal edilmeme için kullanılan kimlik indisleri de dahil olmak üzere, değer atamasını yapar ve kimlik bilgisi ***C***'yi kimlik sahibine verir. Ayrıca kimlik sağlayıcı, indisi iptal edilmeme birikimli değerine ekler.
5. Kimlik talep eden, ε kanıt talebini kimlik sahibine gönderir. Kanıt talebi, kimlik bilgisi şeması ***S*** ve bilgileri açığa çıkarma önermeleri ***D***'yi içerir. Öznitelik m ve değer V için önermeler, $m = V$, $m < V$ veya $m > V$ şeklinde olabilir. Bazı özniteliklerin aynı olup olmadığı $m_i = m_j$ şeklinde de önermeler belirtilebilir.
6. Kimlik sahibi, kimlik bilgisi şeması ***S***'ye karşılık gelen kimlik bilgilerine sahip olup olmadığını kontrol eder ve blok zincirinden iptal edilmemeye ilişkin kanıt bilgisini alır.
7. Kimlik sahibi, iptal edilmemiş bir kimlik bilgisine sahip olduğunu ve kanıt talebi ε'yi karşıladığını gösteren bir kanıt ***P*** oluşturur ve bunu kimlik talep edene gönderir.
8. Kimlik talep eden, gönderilen kanıtı doğrular.

5.5.2. X.509 sertifikaları ile karşılaştırma

Dijital kimlik ve X.509 sertifikalarının verilmesi süreci aşağıdaki bakımlardan birbirilerine çok yakındır:

- Bir dizi öznitelik dijital olarak imzalanır.
- Dijital imza taklit edilemez.
- Dijital olarak imzalanan kimlik bilgisi, kriptografik olarak bir gizli anahtara bağlıdır.

Ancak, Hyperledger Indy'de kullanılan imza şeması, imzanın ve ilgili özniteliklerin mevcudiyetine dair sıfır-bilgi kanıtlarını sağlar ve bunu yaparken imzanın ve öznitelik değerlerinin kendilerini açığa çıkarmaz. X.509 sertifikası kullanıldığında, imzanın doğrulanması için tüm özniteliklerin açığa çıkması gerekir. Bu durum, aynı sertifikanın tüm kullanımlarının birbirine bağlanabilmesine yol açar. Hyperledger Indy'deki imzalarla, kanıtların orijinal kimlik bilgilerine bağlanması mümkün değildir. Ayrıca X.509 sertifikaları merkezi bir sertifika otoritesi tarafından yayınlanır ve yönetilir. Dijital kimliklerde ise, merkezi otoriteye olan bağımlılık daha azdır ve dağıtık yapılar kullanarak kimlik doğrulama işlemleri gerçekleştirilebilir.

5.5.3. Güvenlik analizi

Önerilen modelin güvenlik analizi iki boyutta ele alınmıştır. Öncelikle model bilgi güvenliğinin temel ilkelerine göre analiz edilmiştir. Daha sonra ise modelin bilinen bazı itibar sistemi saldırılarına karşı nasıl koruma sağladığı değerlendirilmiştir.

Bilgi güvenliği boyutu

Modelin bilgi güvenliği açısından analizi, kimlik bilgilerinin mahremiyetini, kimliklerin bağlantılandırılamaz olmasını ve saklanan geri bildirim verisinin bütünlüğünü içermektedir.

Kimlik bilgilerinin mahremiyeti

Kimlik bilgilerinin mahremiyeti, kimlik bilgilerini sunanın gerçek kimliğini diğer varlıkların belirleyememesini gerektirir. Modelimizde, kimlik sahibinin kimliğinin gizliliğinin sağlandığı iki durum vardır: Geri bildirim jetonları için geri bildirim veren alıcının kimliği gizli tutulur ve indirim jetonları için satıcının ve pazar yerinin kimliği gizli tutulur.

5.5.1 bölümünde açıklandığı gibi, modelimiz sıfır bilgi ispatı kullandığından kimlik kanıtları kimlik talep edene sunulduğunda kimlik sahibinin kimlik bilgileri ifşa edilmez. Sıfır bilgi ispatının yanı sıra, modelimizde mahremiyetin korunmasını artıran bir başka mekanizma da kimlikler arası korelasyonu önleyen "bağlantı sırrı" kullanımıdır. Bağlantı sırrı, yalnızca sahibinin kendisi tarafından bilinen gizli bir değere yönelik kör bir kriptografik taahhüttür. Kimlik bilgisi verme sırasında, bağlantı sırrı kimlik sağlayıcıya kör bir öznitelik olarak gönderilir. Bu da kimlik sağlayıcının kimlik sahibini bilmesine engel olur. Kimlik sağlayıcının gizli bağlantı sırrını da içeren her bir özniteliği ayrı ayrı imzalaması, kimlik özniteliklerinin seçimli olarak açıklanmasına veya gizlenmesine olanak tanır. Bu, kimlik sağlayıcının bağlantı sırrının gerçek değeri hakkında hiçbir bilgisi olmadığı ve kimlik sahibinin kimlik bilgilerinin sahipliğini herhangi bir kalıcı kimlik bilgisi ifşa etmeden kimlik talep edene kanıtlayabildiği anlamına gelir. Bağlantı sırrı açık şekilde kimlik sağlayıcılarla, kimlik talep edenlerle veya diğer taraflarla paylaşılmaz. Kötü niyetli bir tarafın bağlantı sırrını türetmek için birden çok farklı gizli bağlantı sırrı değeri kullanması mümkün değildir. Ancak kimlik sahibinin aynı bağlantı sırrının her bir kimlik bilgisine dahil edildiğini kimlik

talep edene kanıtlaması mümkündür. Önerilen modelde sıfır bilgi ispatı ve bağlantı sırlarının kullanımı ile kimlik sahibinin kimliğinin gizliliği sağlanmaktadır.

Veri bütünlüğü

Veri Bütünlüğü, verilerin doğru, tutarlı, güvenilir olmasını ve yetkisiz bir şekilde değiştirilmemiş veya tahrif edilmemiş olmasını gerektirir. Önerilen model, geri bildirim verilerinin bütünlüğünü sağlamak için aşağıdaki mekanizmalara sahip bir blok zinciri kullanır.

Önerilen modelde kullanılan blok zinciri, Hyperledger Fabric, katılımcı düğümlerin işlem verilerinin blok zincirine eklenmeden önce geçerliliği üzerinde anlaşmasını gerektiren bir mutabakat protokolü kullanır. Bu mutabakat mekanizması, tüm düğümlerin blok zincirinde depolanan verilerle ilgili tutarlı bir görünüme sahip olmasını sağlar ve verileri manipüle etmeye yönelik herhangi bir girişim ağ tarafından algılanır ve reddedilir. Ayrıca, kimlik doğrulamayı sağlamak ve yalnızca yetkili katılımcıların ağda işlem yapabilmesini sağlamak için dijital imzalar kullanır. Bu mekanizma, ağı yetkisiz erişime karşı korur ve kötü niyetli kişilerin verileri tahrif etmesini engeller. Ayrıca, aktarılan ve duran verilerin güvenliğini sağlamak için uçtan uca şifreleme sağlar. Bu, verilerin yetkisiz erişime, müdahaleye veya değiştirilmeye karşı korunmasını sağlayarak ek bir güvenlik katmanı sağlar ve verilerin bütünlüğünü sağlar.

Bilinen saldırılara karşı koruma

Önerilen model itibar sistemlerine karşı bazı bilinen saldırılara karşı koruma sağlar.

Kötüleme saldırıları

Kötüleme saldırısının en önemli amacı bir rakibin itibarını düşürmektir (Cai ve Zhu, 2016; Hasan vd., 2020; Schaub vd., 2016). Birçok araştırma, kullanıcıların yalnızca bir satın alma işlemi yaptıktan sonra satıcılar için geri bildirim göndermelerini sınırlamanın, kötüleme saldırılarıyla mücadele etmenin önemli bir yolu olduğunu göstermektedir (Cai ve Zhu, 2016; Koutrouli ve Tsalgatidou, 2012; Schaub vd., 2016). Bu durumda saldırganın olumsuz geri bildirim gönderebilmesi için rakip bir satıcının satışına katkıda bulunması gerekir. Modelimiz, alıcıların geri bildirim gönderebilmeleri için doğrulanabilir kimlik bilgileri

biçiminde geri bildirim jetonuna sahip olmalarını zorunlu kılar. Geri bildirim jetonu, yalnızca bir e-ticaret işleminin tamamlanmasından sonra verilir. Bu nedenle, geri bildirimler ilgili işlemlerle birebir bağlantılıdır ve bu da kötüleme saldırılarının azaltılmasına yardımcı olur.

Sahte oylama saldırıları

Kötüleme saldırılarının önlenmesine benzer şekilde, geri bildirim gönderiminin yalnızca satın alma işlemi gerçekleştiren kullanıcılarla sınırlandırılması da sahte oylama saldırılarına karşı bir önlemdir. Pazar yerlerinde dükkanları olan satıcılar, pazar yerleri satıcılar adına geri bildirim jetonu ürettiğinden, satın alma işlemi gerçekleştirmeden kendileri için geri bildirim gönderemezler. Bu nedenle, geri bildirim jetonları, sahte oylama saldırılarını da azaltmaya yardımcı olur. Ancak, kendi e-ticaret platformlarına sahip satıcılar için, satıcıların kendileri için olumlu geri bildirim göndermelerini sağlayacak sahte jetonlar üretmelerini engellemenin bir yolu yoktur. Chang ve ark. dürüst geri bildirimleri teşvik etmeye yönelik yaklaşımlara ilişkin araştırmalarında, geri bildirim verenlerin mahremiyetinin korunmasının adil geri bildirimler toplamak için önemli bir faktör olduğunu ortaya koydu (Chang vd., 2019). Geri bildirim sağlayan alıcı bilgisinin ifşası, mütekabiliyet gereği haksız yere yüksek olumlu geri bildirimlerle sonuçlanabilir (Resnick, 2002). Modelimizin geri bildirim sağlayan alıcıların gizliliğini koruma özelliği, dürüst olmayan olumlu geri bildirimlerin azaltılmasına yardımcı olur.

Aklama/yeniden giriş saldırıları

Aklama ve yeniden giriş saldırılarını önlemenin bir yolu, bir satıcının kaydını gerçek dünya kimliğine bağlamaktır (Bellini vd., 2020; Koutrouli ve Tsalgatidou, 2012; Schaub vd., 2016). Yasal merciler tarafından verilen dijital kimliklerin zorunlu kılınması, satıcıların sistemdeki kayıtlarıyla ilişkili tüzel kişilik numaralarına sahip olmasını sağlar. Bu nedenle, sistemden çıkmak ve tekrar katılmak, önceki geri bildirimleri ve itibar puanını sıfırlamaz.

Sybil saldırıları

Aklama ve yeniden giriş saldırılarının önlenmesine benzer şekilde, tüzel kişilik numaralarına bağlı dijital kimlikler, tek bir satıcı için birden fazla kimlik oluşturulmasını engeller. Satıcılar, gerçek dünyada kullanılan vergi numarası, ticari sicil numarası gibi numalarla ayırt edilir. Yasal mercilerden birden fazla dijital kimlik alınması, sistemde birden fazla kimlik oluşturulması sonucunu doğurmaz.

İhanet saldırıları

Hasan ve diğerlerinin belirttiği gibi, itibar puanı hesaplanırken geri bildirimlerin verildiği tarih ile satın alma işleminin yapıldığı tarih arasında ne kadar süre geçtiğine göre geri bildirim puanlarının ağırlıkları dikkate alınarak hesaplanmasıyla bu saldırı azaltılabilir (Hasan vd., 2020). Modelimizde yer alan itibar puanı hesaplama algoritması, geri bildirim puanlarını geçen süreye ve işlem tutarına göre ağırlıklandırır. Bu nedenle, modelimizdeki algoritma ihanet saldırılarını azaltmaya yardımcı olur.

5.6. Modelin Performansı

Önerdiğimiz itibar sistemi, mevcut e-ticaret platformları ile birlikte çalışabilen ve REST API'ler aracılığıyla sistemlerle entegrasyona izin veren bir yapıya sahiptir. İtibar sistemimiz bir e-ticaret platformuyla entegre edildiğinde, blok zinciri kullanarak sağladığı güvenlik ve mahremiyet faydalarının yanında sisteme bazı ek yükler de getirir. Bu bölümde, sistemin e-ticaret sistemlerine entegre edilebilirliği bakımından yapılan testleri ve buna yönelik bir uygunluk değerlendirmesi sunulmaktadır. Çeşitli test senaryolarına dayalı olarak sistemde ortaya çıkan gecikmeleri ve blok zincirinde oluşan blokların boyutlarını test etmek amacıyla bulut hizmet sağlayıcılarından birinde çalışan iki sunucu oluşturulmuştur.

DKS Sunucusu, Doğrulanabilir Kimlik Alt Sistemi için gerekli olan tüm Docker konteynerlerini çalıştırır. Bu sunucu, üzerinde 16GB RAM ve 4 vCPU olan Ubuntu 20.04 LTS kurulu bir Linux sunucudur. Bu sunucunun ana görevi Hyperledger Indy blok zinciri ağı ile birlikte bu ağ ile iletişim kuran dijital kimlik vekil yazılımlarını barındırmaktır. Bu sunucu aşağıdaki Docker konteynerleri çalıştırır:

- Hyperledger Indy blok zinciri ağı kurmak için dört konteyner
- Hyperledger Indy blok zinciri ağını izlemek için bir konteyner

- Alıcıyı, satıcıyı, yasal merciyi ve geri bildirim toplama alt sistemini temsil eden ve Hyperledger Indy blok zinciri ağı ile iletişim kuran dört vekil yazılım konteyneri

GTS Sunucusu, Geri Bildirim Toplama Alt Sistemi için gerekli olan tüm Docker konteynerlerini çalıştırır. Bu sunucu, üzerinde 16GB RAM ve 4 vCPU olan Ubuntu 20.04 LTS kurulu bir Linux sunucudur. Bu sunucunun ana görevi, üzerinde akıllı kontratların yüklendiği bir Hyperledger Fabric blok zinciri ağını sağlamaktır. Bu sunucu aşağıdaki Docker konteynerleri çalıştırır:

- Yasal merci, satıcı ve geri bildirim toplama alt sisteminin her biri için beş konteyner: eş düğümler için iki konteyner, akıllı kontratlar için iki konteyner ve sertifika sunucusu için bir konteyner
- Sıralayıcı düğümler için üç konteyner

Hyperledger Fabric ve Hyperledger Indy blok zinciri ağlarının ve vekil yazılımların DKS ve GTS sunucuları üzerine kurulması işlemlerinin yanı sıra, iki temel yazılım parçasının geliştirmesi yapılmıştır.

1. Hyperledger Fabric blok zinciri ağında çalışan akıllı kontrat yazılımlarının geliştirmesi yapılmıştır. Hyperledger Fabric SDK Java, Go ve Node (JavaScript/TypeScript) programlama dilleri ile akıllı kontrat yazmayı desteklemektedir. Bu çalışma kapsamındaki akıllı kontratlar TypeScript programlama dili kullanılarak yazılmıştır. Yazılan akıllı kontratlar Hyperledger Fabric komutları ile blok zinciri ağındaki tüm düğümlere yüklenmiştir.
2. Blok zincirindeki akıllı kontratlarla haberleşmeyi sağlayan REST mimarisine sahip web servislerinin geliştirmesi yapılmıştır. Bu web servisleri, itibar sistemi ile e-ticaret platformlarının ve diğer paydaşlara ait sistemlerin entegre olmasını sağlayan ara yüzler sunmaktadır. Akıllı kontratlarla doğrudan haberleşme ihtiyacını ortadan kaldıran ve kolay bir entegrasyon ara yüzü sunan bu web servisleri de TypeScript programlama dili kullanılarak yazılmıştır. Bu web servisleri Node.js web sunucu yazılımı üzerinde çalıştırılmıştır.

Sistemin performans ölçümlerini yapmak amacıyla REST web servislerine istekler gönderilmiş ve her aşamada geçen süreler log kayıtlarına yazılarak izlenmiştir. REST web servislerine istek göndermek amacıyla Postman API test aracı kullanılmıştır.

Yapılan testlerde elde edilen sonuçlar aşağıda verilmiştir.

Doğrulanabilir kimlikler ile ilgili mesaj alışverişleri, e-ticaret sürecinin çeşitli aşamalarında gerçekleşse de tüm doğrulanabilir kimlik mesaj alışverişleri birbirine çok yakın gecikme değerlerine sahiptir. Aşağıdaki tabloda testlerde gözlemlenen ortalama gecikme değerleri ile bu mesaj alışverişlerinin türleri listelenmektedir. Bu gecikme değerleri, daha sonra belli e-ticaret süreçleri için sistemin genel yükünü hesaplamak için kullanılacaktır. Ortalama gecikme değerleri her bir mesaj alışveriş türü için en az 30 test durumu çalıştırılarak elde edilmiştir.

Çizelge 5.1. Doğrulanabilir kimlik mesaj alışverişleri

Mesaj Alışveriş Türü	Test Durumları	Ortalama Gecikme
Kimlik Sağlama	Dijital Kimlik (*YM'den S'ye*) Geri Bildirim Jetonu (*S'den* A'ya) İndirim Jetonu (*GTS'den A'ya*)	172ms
Kanıt Talebi	Dijital Kimlik (*GTS'den S'ye*) Geri Bildirim Jetonu (*GTS'den* A'ya) İndirim Jetonu (*S'den A'ya*)	115ms
Kanıt Gönderme	Dijital Kimlik (*S'den GTS'ye*) Geri Bildirim Jetonu (*A'dan* GTS'ye) İndirim Jetonu (*A'dan S'ye*)	165ms

Satıcı Kayıt Fazı, diğer e-ticaret faaliyetlerinden bağımsız bir aşamadır ve satın alma işlemlerinden ve geri bildirim gönderimlerinden tamamen izoledir. Bu nedenle, Satıcı kayıt aşamasındaki herhangi bir gecikmenin diğer e-ticaret faaliyetleri üzerinde bir etkisi yoktur. Ancak, bu aşama ek adımlar getirdiğinden, yine de bu aşamayla ilgili metrikler aşağıda verilmiştir.

Çizelge 5.2. Satıcı kayıt fazı metrikleri

#	Adım	Ortalama Gecikme
1	Dijital Kimlik Verilmesi (YM'den S'ye)	172ms
2	Dijital Kimliğin Kanıtının Talep Edilmesi (GTS'den S'ye)	115ms
3	Kimlik Kanıtının Gönderilmesi (S'den GTS'ye)	165ms
4	Dijital Kimliğin Doğrulanması ve Satıcının Blok Zincirine Eklenmesi	2437ms
	Toplam	2889ms

Alışveriş Fazı, satın alma işlemi ile sistemde bir sipariş oluşturulduktan sonra ***S***'nin ***A***'ya geri bildirim jetonu vermesini içerir. Ancak, geri bildirim jetonu vermek, satın alma işleminin bir parçası değildir ve bu işlemin süresini uzatmaz. Bir satın alma işlemi tamamlandığında, itibar sisteminin bir parçası olan mesaj kuyruğuna bir mesaj yerleştirilir ve mesaj, satın alma işlemi kesintiye uğramadan asenkron olarak işlenir. Mesaj işlendiğinde, Çizelge 5.2'de gösterildiği gibi, ***A***'ya geri bildirim jetonu verilmesi 172 ms sürer. Alışveriş fazındaki bir başka olası kullanıcı davranışı, ***S***'nin performansı ve güvenilirliği hakkında fikir sahibi olmak için belirli bir ***S***'nin geri bildirimlerini çekmektir. Geri bildirimleri çekme fonksiyonunu blok zincirinde saklanan çeşitli boyutlarda geri bildirim verilerine sahip bir ***S*** için test ettik. Çizelge 5.3, saklanan geri bildirimlerin boyutuna bağlı olarak değişen yanıt sürelerini göstermektedir.

Çizelge 5.3. Satıcı geri bildirimlerini çekme yanıt süreleri

Geri Bildirim Veri Boyutu	Yanıt Süresi
1KB	180 ms
2KB	250 ms
3KB	218 ms
4KB	276 ms
8KB	227 ms
16KB	241 ms
26KB	269 ms
32KB	301 ms
66KB	214 ms
132KB	440 ms
176KB	382 ms
264KB	562 ms
440KB	810 ms
768KB	1496 ms
1034KB	2109 ms

Çizelge 5.3'te görüldüğü gibi, saklanan geri bildirim kayıtlarının boyutu arttıkça yanıt süresi de artar. Bu beklenen bir davranıştır. Ancak sadece bir satıcı için yaklaşık 1MB geri bildirim içeren testin yanıt süresi bile 2,1 saniyeyi geçmemektedir. Blok zincirinden geri bildirim kayıtlarını çekmek için geçen yanıt sürelerini, itibar sisteminin e-ticaret sistemlerine entegrasyonu bakımından kabul edilebilir süreler olarak değerlendirmekteyiz.

Hizmet sunumu fazı performans ölçümlerinde yer almamaktadır. Çünkü hizmet sunum fazı, sistem üzerinde gerçekleşen bir faz olmayıp satıcının alıcıya mal veya hizmeti fiziksel olarak ulaştırması aşamasıdır. Bu nedenle performans ölçümlerinde hizmet sunum fazına ilişkin bir kayıt bulunmamaktadır.

Geri Bildirim Fazı, ***A***'nın ***S*** için geri bildirimleri ***GTS***'ye göndermesi, ***GTS***'nin geri bildirimleri blok zincirinde saklaması ve hesaplamaları gerçekleştirmesi ile ilgili tüm adımları içerir. Bu aşama için ***A***'nın ***S***'den geri bildirim jetonu almış olması bir ön koşuldur.

Çizelge 5.4. Geri bildirim fazı metrikleri

#	Adım	Ortalama Süre
1	Geri Bildirim Jetonu Kanıtının Talep Edilmesi (GTS'den A'ya)	115ms
2	Kanıtın Gönderilmesi (A'dan GTS'ye)	165ms
3	Kanıtın Doğrulanması, Geri Bildirimin Blok Zincirine Eklenmesi ve İtibar Puanının Hesaplanması	2540ms
4	İndirim Jetonu Verilmesi (GTS'den A'ya)	172ms
	Toplam	2992ms

Geri bildirim fazının üçüncü adımı olan kanıtın doğrulanması, geri bildirimin blok zincirine eklenmesi ve itibar puanının hesaplanması adımını ***A*** tarafından gönderilen farklı boyutlardaki geri bildirim mesajlarıyla daha detaylı test ederek aşağıdaki sonuçlara ulaştık.

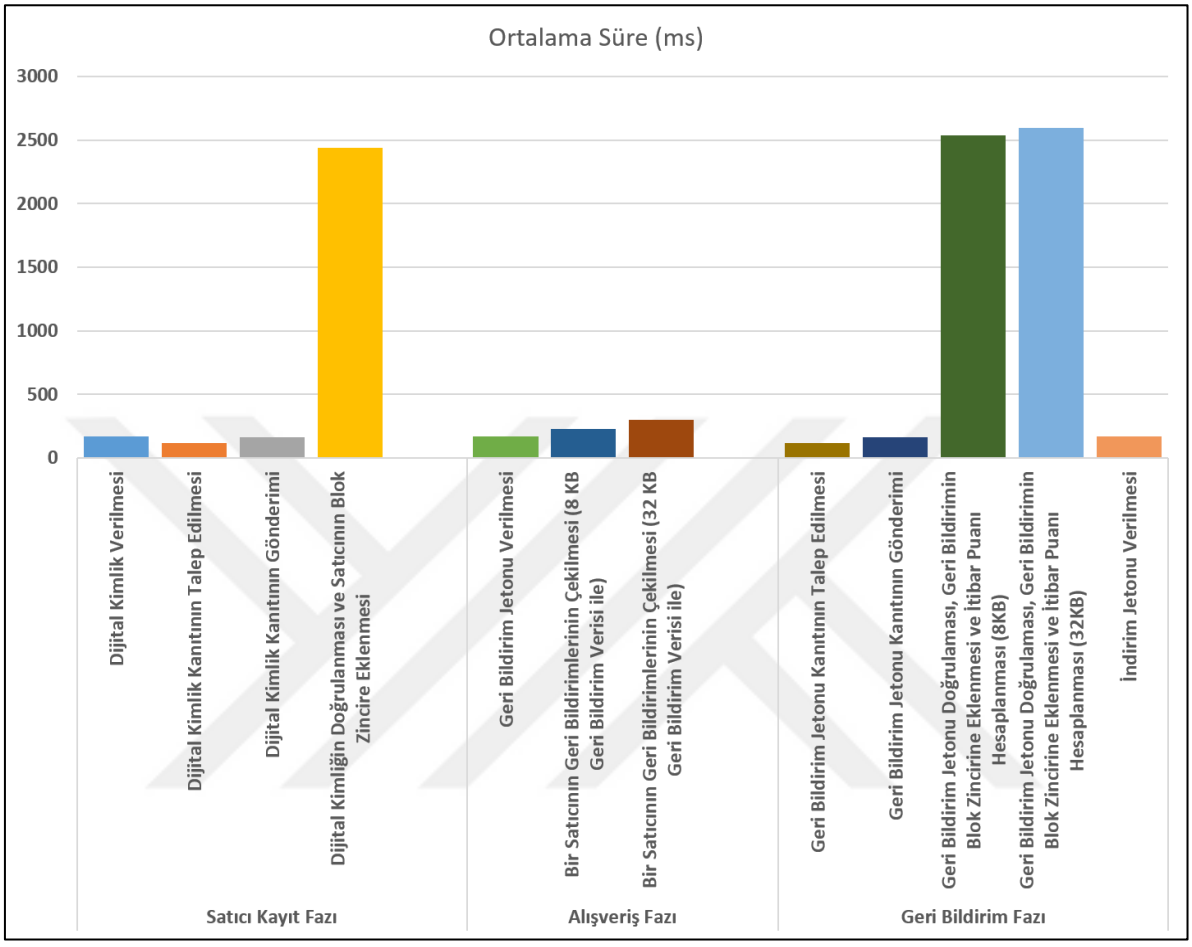
Çizelge 5.5. Kanıtın doğrulanması, geri bildirimin blok zincirine eklenmesi ve itibar puanının hesaplanması

Geri Bildirim Mesajı Boyutu	Yanıt Süresi	Blok Zincirinde Oluşturulan Blok Boyutu
125B	2471ms	6K
250B	2518ms	6K
500B	2519ms	7K
1KB	2577ms	8KB
2KB	2504ms	10KB
4KB	2502ms	14KB
8KB	2540ms	22KB
16KB	2648ms	38KB
24KB	2548ms	54KB
32KB	2599ms	70KB

Çizelge 5.5'te görüldüğü gibi, geri bildirim mesajının boyutunun, geri bildirim gönderme işlevinin yanıt süresi üzerinde önemli bir etkisi yoktur. Bununla birlikte, Hyperledger Fabric blok zincirinde oluşturulan bloğun boyutu, geri bildirim mesajının boyutu arttıkça artar ki bu beklenen bir davranıştır.

Sistemimizin e-ticaret sürecinin her aşaması üzerindeki genel etkisi aşağıdaki şekilde gösterilmiştir. Şekilde görüldüğü gibi, kimlik bilgilerinin verilmesi, kanıt talepleri ve kanıtların gönderilmesi işlemleri çok az gecikmeye sebep olurlar. Gecikme süresinin en

yüksek olduğu adımlar, kimlik bilgilerinin doğrulanmasını ve blok zincirine veri eklenmesini içeren adımlardır.



Şekil 5.5. Her bir adımın ortalama gecikme süresi

6. SONUÇ VE ÖNERİLER

Bu tez çalışması ile e-ticaret işlemlerinde güveni artırmak amacıyla blok zinciri kullanan çözüm önerileri getirilmiştir. Bu önerilerden ilki, e-ticarete özgü kapsamlı bir dijital kimlik güven çerçevesi önerisidir. Dijital kimliklerle ve dijital kimlik güven çerçevesiyle ilgili gerçekleştirilmiş olan mevcut çalışmalar incelendiğinde, bu çalışmalarda daha çok kişilerin ulusal düzeyde dijital kimlik kullanımına ve kamu kurumlarının sağladığı çevrim içi hizmetlere bu yolla erişmelerine yönelik düzenlemelere ve çözüm önerilerine ağırlık verildiği görülmektedir. Bu tez çalışmasında ise dijital kimliklerin ve dijital kimlik güven çerçevesinin e-ticaret alanına özelleştirilmiş şekilde güven artırıcı çözümler sunan bir kullanım alanına odaklanılmıştır. Bu kapsamda önerilen dijital kimlik güven çerçevesi modeli, alıcıların e-ticaret işlemlerinde kendilerini daha güvende hissetmelerini, satıcı ve üretici firmalara daha fazla güven duymalarını sağlamaya yönelik olarak tasarlanmıştır. Araştırmalarımızda dijital kimlik güven çerçevesinin e-ticaret işlemlerinde, bu çalışmadaki bağlamda kullanımına yönelik Türkiye'de ve yurt dışında bir çalışmaya rastlanmamıştır. Bu çalışmada önerilen dijital kimlik güven çerçevesi, e-ticaret ekosisteminin paydaşlarını içine alan, güven çerçevesi kapsamını prensipler, yönetim şeması, standartlar, kurallar, işleyiş ve yönetişim yönleriyle ele alan bir model ortaya koymaktadır.

Bu çalışmada önerilen dijital kimlik güven çerçevesi modeli, öncelikle modelin temel alacağı ilkeleri ortaya koymuş ve bu ilkeleri modelin bir parçası haline getirmiştir. Önerilen model belirlenen ilkeleri temel alan bir modeldir. Bu ilkelerden biri, şirketlerin kendi dijital kimlikleri ya da dijital kimliklerinde bulunan bilgileri tamamen veya kısmen paylaşma veya paylaşmama kontrolünün kendilerinde olmasıdır. Bu nedenle güven çerçevesinin dijital kimlik yönetim şeması dağıtık veya diğer bir ifadeyle kullanıcı egemen kimlik yönetim şeması olarak belirlenmiştir. Bu kimlik yönetim şeması kullanıldığında kuruluşlar tüm temel ve bağlamsal kimliklerini kendilerine ait dijital cüzdanlarda saklarlar. Ayrıca kendi sakladıkları bu dijital kimliklerin veya dijital kimliklerinde bulunan bilgilerin tamamen veya kısmen paylaşımı konusunda tam kontrole sahip olurlar. Belge sahibi bir kuruluşun o belgeye sahip olduğunu ve belgenin halen geçerli olduğunu kanıtlamak için o belgenin veya belgedeki bilgilerin tamamını paylaşması şart değildir. Belge sahibinin sadece gerekli bilgileri paylaşması ve diğer bilgileri paylaşmaması, belgede bulunan kişisel verilerin gereksiz yere başkalarına aktarılmasını önlemiş olacaktır. Bu nedenle, önerilen dijital kimlik

güven çerçevesi modelinin Kişisel Verileri Koruma Kanunu (KVKK) düzenlemesine uyumlu ve kişisel verilerin korunmasını destekleyen bir model olduğu söylenebilir.

Bu çalışmada önerilen dijital kimlik güven çerçevesi Türkiye'de halen uygulanmakta olan Güven Damgası ile benzer bir amaca hizmet etmektedir. Güven Damgası da e-ticaret firmalarının belli şartları sağladığının bir göstergesi olarak, müşterilerin bu firmalara daha fazla güven duymasını hedefleyen bir uygulamadır. Güven damgası firmaların çok dar bir kapsamda uyması gereken şartları belirlemiş, sadece bir kısım siber güvenlik önlemlerine sahip olmaları ve e-ticaret hizmetlerini birtakım kurallar çerçevesinde yürütmeleri konusunda kurallar koymuştur. Dijital kimlik güven çerçevesi ise konuyu güven damgasının çok ötesinde bir kapsamla ele almakta, firmaların temel dijital kimlikleri, sertifikaları, yetki belgeleri, akreditasyon ve uygunluk belgeleri, güven damgası gibi tüm belgelerin geçerliliğini ve yetkili kuruluşlar tarafından verildiğini kanıtlayan blok zinciri tabanlı dijital kimliklerin kullanımına ilişkin bir model sunmaktadır. Güven çerçevesinde tanımlı kural ve düzenlemelere uyan paydaşlara da Dijital Kimlik Güven Çerçevesi Güven İşareti vererek bu paydaşlara duyulan güveni artırmayı hedeflemektedir.

Bu tez çalışmasında önerilen dijital kimlik güven çerçevesinin hayata geçirilebilmesi için bir takım yasal düzenlemelere ihtiyaç vardır. Türkiye'de dijital kimlik güven çerçevesi konusuna en yakın yasal düzenleme, 2004 yılında çıkarılan 5070 sayılı Elektronik İmza Kanunu ve ilgili yönetmeliklerdir. Bu düzenlemeler, ülkemizde elektronik imzanın yasal olarak kabul edilmesine olanak sağlamıştır. Blok zinciri tabanlı dijital kimlik alt yapısı teknolojik olarak yüksek seviyede güvenlik sağlasa da mevcut düzenlemeler dijital kimliklerin yasal olarak geçerli sayılabilmesi için yeterli değildir. Çünkü mevcut yasal düzenlemeler elektronik sertifika hizmet sağlayıcısı olarak yetkilendirilmiş kuruluşların sertifikalarını ve zaman damgasını zorunlu kılar. İhtiyaç duyulan yasal düzenlemelerin diğer bir diğer boyutu da kamu kurumlarının dijital kimlik sağlayıcısı olarak güven çerçevesinde yer alabilmeleri için gereken düzenlemelerdir. Ayrıca güven damgası için TOBB'un yetkilendirildiği gibi, güven çerçevesindeki rollerden değerlendirme ve denetleme kuruluşlarının da güven çerçevesi kapsamında yetkilendirilmeleri gerekmektedir.

Bu tez çalışması kapsamında önerilen dijital kimlik güven çerçevesi, Türkiye'deki yasal düzenlemeler ve uygulamalar özelinde ele alınmış ve e-ticaret sektörüne yönelik olarak özelleştirilmiştir. Bunun yanında güven çerçevesinin ilkeleri, dijital kimlik yönetim şeması,

dijital kimlik veri yapısı, dijital kimlik ibrazı ve doğrulama ile güven işareti gerekli uyarlamaların yapılmasıyla farklı sektörlere ve ülkelere uygun hale getirilebilir. Örneğin önerilen güven çerçevesi kapsamındaki kimlik ispatı ve dijital kimlik alma sürecinin Türkiye'ye özgü yanı, Türkiye'deki mevzuatla düzenlenen EKDS'nin kullanılmasını içermesidir. Ayrıca temel ve bağlamsal dijital kimlikler de Türkiye'deki mevzuatın zorunlu kıldığı ve e-ticaret sektörü için gerekli olan belgeleri temel almıştır. Fakat farklı ülkelerdeki düzenlemeler ve uygulamalar ile farklı sektörler göz önünde bulundurularak kimlik ispat yöntemleri, dijital kimlik yapısı ve çeşitleri ile diğer güven çerçevesi unsurları farklı ülkeler ve sektörler için uygun hale getirilebilir.

E-ticaret işlemlerinde güvenin artırılmasına yönelik getirilen diğer bir öneri ise blok zinciri temelli ve mahremiyet odaklı bir itibar sistemi önerisidir. İtibar sistemi, kullanıcıların mahremiyetini koruyan, kötücül saldırılara karşı korunaklı ve güvenli bir sistem oluşturmayı amaçlayan iki alt sistemden oluşmaktadır. Bunlardan ilki, uçtan uca doğrulanabilir bir kimlik bilgisi düzenleme ve doğrulama altyapısı sağlamayı amaçlayan Doğrulanabilir Kimlik Bilgileri Alt Sistemidir. İkinci alt sistem ise, amacı alıcıların geçerli bir geri bildirim jetonuna sahip olduklarını doğruladıktan sonra alıcılardan geri bildirim almak, özgün olarak geliştirdiğimiz algoritmamızı kullanarak itibar puanını hesaplamak ve satıcılar ile pazar yerleri adına indirim jetonları vermek olan Geri Bildirim Toplama Alt Sistemidir.

Sistemi blok zinciri teknolojisi üzerine inşa etmek, doğal olarak merkezi olmayan, değiştirilmelere ve saldırılara karşı güvenli bir altyapı katmanı sağlamaktadır. Önerilen itibar sisteminde blok zinciri teknolojisi olarak, açık blok zincirlerine kıyasla yüksek performanslı bir platform sağlayan, verimli mutabakat mekanizmalarına sahip özel bir blok zinciri alt yapısı olan Hyperledger Fabric seçilmiştir. Doğrulanabilir kimlik kavramının ve buna ilişkin W3C standardının, satıcıların dijital kimlikleri ve gerçekleştirilen e-ticaret işlemlerinin ve geri bildirim gönderimlerinin kanıtları olarak sisteme entegre edilmesi, önerdiğimiz itibar sistemini yenilikçi bir hale getirmektedir. Doğrulanabilir kimlik bilgilerinin uygulanması için Hyperledger Indy blok zincirinin kullanılması, sağlam bir dijital kimlik alt yapısı ve sıfır bilgi ispatı gibi ek yetenekler sağlamaktadır. Sıfır bilgi ispatları, sistemimizin alıcıların gizliliğini koruyarak kullanıcıları dürüst geri bildirimler göndermeye teşvik etmesini sağlar. Bölüm 5.5'te açıklandığı gibi sistemin güvenlik analizi, sistemin geri bildirim gönderenlerin kimliklerinin gizliliğini koruduğunu ve geri bildirim verilerinin bütünlüğünü sağladığını göstermektedir. Geri bildirim gönderimlerini yalnızca satın alan kullanıcılarla

sınırlandırmak, kötüleme ve sahte oylama saldırılarına karşı etkili bir korumadır. Dürüst geri bildirimleri sağlamak için itibar sistemimizin getirdiği bir başka önlem ise geri bildirim gönderimlerinin sonucunda verilen indirim jetonlarıdır. Satıcıların yasal kimliklerini dijital kimliklere bağlamak, aklama/yeniden giriş ve Sybil saldırıları gibi kimlikle ilgili saldırıları önlemeye yardımcı olur. Tüm bu özelliklere sahip itibar sistemimiz itibar sistemlerine yönelik 5.5.3 bölümünde sıralanan saldırılara karşı güvenlik önlemleri sağlamaktadır.

Sistemin özel bir blok zinciri olan Hyperledger Fabric kullanılarak gerçekleştirilmesi ile verilerin saldırılarla değiştirilmesine dayanıklılık konusunda iyileştirme sağlanmıştır. Merkezi sistemlerde tek bir noktaya yapılan başarılı bir saldırı ile sistemdeki verilerin değiştirilmesi mümkün iken Hyperledger Fabric blok zinciri ile tüm düğümlerin en az üçte birinin kötücül olduğu durumda veri değiştirmek mümkün olabilmektedir. Örneğin itibar sistemimizin dokuz düğümden oluştuğu bir senaryoda ancak en az üç düğümün kötücül saldırıyla ele geçirilmesi durumunda sistemdeki verilerin saldırı sonucu değiştirilmesi mümkündür. İtibar sistemini oluşturan düğüm sayısı arttıkça, kötücül saldırıyla ele geçirilmesi gereken düğüm sayısı da artmaktadır. Merkezi sistemlerdeki "tek başarısızlık noktası" sorunu blok zinciri ile ortadan kalkmakta ve toplam düğüm sayısının en az üçte biri kötücül olduğunda başarısızlık olabilmektedir.

Hyperledger Fabric kullanımının Bitcoin veya Ethereum gibi açık blok zincirlerine nazaran getirdiği bir diğer iyileştirme alanı ise bir saniyede gerçekleştirilen işlem sayısıdır. Huaqun ve Xingjie'nin yaptığı çalışmada bir saniyede gerçekleşen işlem sayısı Bitcoin ağında en fazla 27 işlem, Ethereum ağında ise 15 işlem olarak gözlemlenirken Hyperledger Fabric ağından bir saniyede 3500 civarında işlem gerçekleşebilmektedir (2022). Bu değerlere göre itibar sistemimiz Bitcoin veya Ethereum üzerinde çalışan itibar sistemlerine göre birim zamanda 100 kattan fazla işlem gerçekleştirebilmektedir. Transaction per Second (TPS) olarak ifade edilen saniyedeki işlem sayısı ölçümünde izinli blok zinciri kullanan itibar sistemimiz, açık blok zinciri kullanan itibar sistemlerine göre çok daha yüksek performans göstermektedir. Yine aynı çalışmada yer alan blokların oluşma süresi Bitcoin'de 6000 saniye, Ethereum'da 15 saniye iken Hyperledger Fabric'te saniye mertebesindedir. Bu verilere göre itibar sistemimizde işlemlerin bloklara yazılması sonrasında blok oluşma süresi, açık blok zincirlerle geliştirilen itibar sistemlerine göre en az 15 kat daha hızlıdır.

Ayrıca, tez çalışması kapsamında önerilen itibar sisteminin yazılım geliştirmesi yapılarak bulut tabanlı sunucularda konuşlandırılmıştır. Bu sunucular üzerinde çeşitli test senaryolarına dayalı testler koşularak sistemin performans değerlendirmesi gerçekleştirilmiştir. Yapılan testlerin sonuçları, önerilen sistemin mevcut e-ticaret ekosistemine uygulanmasının ve entegre edilmesinin oldukça uygulanabilir olduğunu göstermektedir.

KAYNAKLAR

Ahn, J., Park, M., Shin, H. ve Paek, J. (2019). A model for deriving trust and reputation on blockchain-based e-payment system. *Applied Sciences*, 9(24), 5362. doi: 10.3390/app9245362

Akram, M. ve Sen, A. (2022). A case study Evaluation of Blockchain for digital identity verification and management in BFSI using Zero-Knowledge Proof. *2022 International Conference on Decision Aid Sciences and Applications (DASA)*, (s. 1295-1299).

Almasoud, A. (2020). *Smart contracts for blockchain-based reputation systems*, Yayımlanmamış Doktora Tezi, University of Technology Sydney, Avustralya.

Almasoud, A., Hussain, F. ve Hussain, O. (2020). Smart contracts for blockchain-based reputation systems: A systematic literature review. *Journal of Net-work and Computer Applications*, 170, 102814.

Amiri, M. J., Allard, T., Agrawal, D. ve Abbadi, A. E. (2022). PReVer: Towards private regulated verified data. *OpenProceedings*, (2), 454-461. doi:10.48786/EDBT.2022.40

Andrade, G. (2019). *Technical analysis of reputation systems based on blockchain Technologies*, Yayımlanmamış Lisans Tezi, Hochschule für angewandte Wissenschaften, Hamburg.

Argento, L., Buccafurri, F., Furfaro, A., Graziano, S., Guzzo, A., Lax, G., . . . Saccà, D. (2020). ID-service: A blockchain-based platform to support digital-identity-aware service accountability. *Applied Sciences*, 11(1), 165. doi: 10.3390/app11010165

Bankalarca Kullanılacak Uzaktan Kimlik Tespiti Yöntemlerine ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasına İlişkin Yönetmelik. (2021, 4 Ocak). *Resmi Gazete*.

Basili, M. ve Rossi, M. (2020). Platform-mediated reputation systems in the sharing economy and incentives to provide service quality: The case of ridesharing services. *Electronic Commerce Research and Applications*, 39, 100835.

Battah, A., Iraqi, Y. ve Damiani, E. (2021). Blockchain-based reputation systems: Implementation challenges and mitigation. *Electronics*, 10(3), 289. doi: 10.3390/electronics10030289

BCTR (2019). *Dijital kimlik raporu*. İstanbul: Blockchain Türkiye Platformu.

Bellini, E., Iraqi, Y. ve Damiani, E. (2020). Blockchain-based distributed trust and reputation management systems: A survey. *IEEE Access*, 8, 21127-21151.

Birleşmiş Milletler (BM) (2020). *Digital identity for trade and development: TrainForTrade case studies in South-East Asia*. TrainForTrade Programme of the United Nations Conference on Trade and Development (UNCTAD)'da sunuldu. Birleşmiş Milletler.

Buechler, M. D. ve Hockenbrocht, C. (2015). Decentralized reputation system for transaction networks. Pensilvanya.

Cai, Y. ve Zhu, D. (2016). Fraud detections for online businesses: A perspective from blockchain technology. *Financial Innovation*, 2(1), 20. doi: 10.1186/s40854-016-0039-4

Camenisch, J. (2010). Specification of the identity mixer cryptographic library. Zurich: IBM Research.

Camenisch, J. ve Lysyanskaya, A. (2003). A signature scheme with efficient protocols, in security in communication networks (2576. Cilt). S. Cimato, G. Persiano ve C. Galdi (Ed.), Berlin, Heidelberg: Springer Berlin Heidelberg, s. 268–289.

Carboni, D. (2015). *Feedback based Reputation on top of the Bitcoin Blockchain*. Pula: CoRR.

Casino, F., Dasaklis, T. K. ve Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, 36, 55–81. doi:10.1016/j.tele.2018.11.006

Chang, J., Xiao, L. ve Xu, W. (2019). A survey of approaches for promoting honest recommendations in reputation systems. *Computer Engineering and Technology*, 179-191.

Dhakal, A. ve Cui, X. D. (2019). *DTrust: A decentralized reputation system for e-commerce marketplaces*. Wuhan.

Dissanayake, K., Somarathne, P., Fernando, U., Pathmasiri, D., Liyanapathirana, C. ve Rupasinghe, D. L. (2021). "Trust pass" - blockchain-based trusted digital identity platform towards digital transformation. *2021 2nd International Informatics and Software Engineering Conference (IISEC)*, (s. 1-6).

Elektronik Ticarette Güven Damgası Hakkında Tebliğ. (2017, 6 Haziran). *Resmi Gazete.*

European Union. (2014). Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. *Official Journal of the European Union*, (257), 73-114.

Fekete, D. L. ve Kiss, A. (2021). A survey of ledger technology-based databases. *Future Internet*, 13(8), 197. doi:10.3390/fi13080197

Gada, S., Dhuri, A., Jain, D., Bansod, S. ve Toradmalle, D. (2021). *Blockchain-based crowdfunding: A trust building model*. 2021 International Conference on Artificial Intelligence and Machine Vision (AIMV)' da sunuldu.

Goldwasser, S., Micali, S. ve Rackoff, C. (1985). The knowledge complexity of interactive proof-systems. *Proceedings Of The Seventeenth Annual ACM Symposium on Theory of Computing*, 291-304.

Goodell, G. ve Aste, T. (2019). Decentralized digital identity architecture. *Front. Blockchain*, 2-17.

Groth, J. (2010). Short pairing-based non-interactive zero-knowledge arguments. *Advances in Cryptology – ASIACRYPT*, 321-340.

Gruner, A., Muhle, A., Gayvoronskaya, T. ve Meinel, C. (2018). A Quantifiable Trust Model for Blockchain-Based Identity Management. *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 1475–1482.

Hasan, O., Brunie, L. ve Bertino, E. (2020). *Privacy preserving reputation systems based on blockchain and other cryptographic building blocks: A survey*.

Huaqun G., Xingjie Y. (2022). *A survey on blockchain technology and its security*. 3-2, doi: 10.1016/j.bcra.2022.100067

İnternet: AccessNow. (2018). National digital identity programmes: What's next? *Access Now*. URL: https://www.accessnow.org/wp-content/uploads/2019/11/Digital-Identity-Paper-Nov-2019.pdf, Son Erişim Tarihi: 17.03.2023.

İnternet: CESG. (2012). GPG 43: Requirements for secure delivery of online public services. CESG – National Technical Authority for Information Assurance. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/270964/GPG_43_RSDOPS_issue_1.1_Dec-2012.pdf, Son Erişim Tarihi: 20.03.2023.

İnternet: CESG. (2013). GPG 44: Using authenticators to protect an online service. CESG - National Technical Authority for Information Assurance. https://www.gov.uk/government/publications/authentication-credentials-for-online-government-services, Son Erişim Tarihi: 20.03.2023.

İnternet: CESG. (2013). GPG 46: Organisation identity. CESG - National Technical Authority for Information Assurance. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/271278/Good_practice_guide_organisation_identity.pdf, Son Erişim Tarihi: 20.03.2023.

İnternet: CESG. (2014). GPG 45: How to prove and verify someone's identity. CESG - National Technical Authority for Information Assurance. https://www.gov.uk/government/publications/identity-proofing-and-verification-of-an-individual, Son Erişim Tarihi: 20.03.2023.

İnternet: DIACC. (2020). Pan-Canadian trust framework glossary. The Digital Identification and Authentication Council of Canada. https://diacc.ca/wp-content/uploads/2020/09/PCTF-Glossary-Final-Recommendation_V1.0.pdf, Son Erişim Tarihi: 20.03.2023.

İnternet: Dünya Bankası (DB) (2018). *G20 digital identity onboarding*. The World Bank Group. https://www.gpfi.org/sites/gpfi/files/documents/G20_Digital_Identity_Onboarding.pdf, Son Erişim Tarihi: 20.03.2023.

İnternet: Dünya Bankası DB (2019). *Practitioner's guide*. The World Bank Group. https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf, Son Erişim Tarihi: 20.03.2023.

İnternet: Dünya Ekonomik Formu (DEF) (2018). *Identity in a digital world*. World Economic Forum. https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf, Son Erişim Tarihi: 20.03.2023.

İnternet: Dünya Ekonomik Formu (DEF) (2019). *Digital identity*. World Economic Forum. https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf Son Erişim Tarihi: 20.03.2023.

İnternet: ID2020. (2018). Manifesto. Web: https://id2020.org/manifesto, Son Erişim Tarihi: 20.03.2023.

İnternet: ID2020. (2019). ID2020 technical requirements. ID2020. https://id2020.org/uploads/files/Technical-Requirements.pdf, Son Erişim Tarihi: 20.03.2023.

İnternet: Lodder, M. ve Khovratovich, D. (t.y.). Anonymous credentials 2.0. https://wiki.hyperledger.org/download/attachments/6426712/Anoncreds2.1.pdf, Son Erişim Tarihi: 20.03.2023.

İnternet: Maler, E., Nadalin, A., Reed, D., Rundle, M. ve Thibeau, D. (2010). *Open identity trust framework (OITF) model*. Open Identity Exchange. https://openidentityexchange.org /user_assets/80.pdf, Son Erişim Tarihi: 20.03.2023.

İnternet: Mothershaw, N. (2020). *OIX guide to trust frameworks*. Open Identity Exchange. https://openidentityexchange.org/user_assets/365.pdf, Son Erişim Tarihi: 20.03.2023.

İnternet: Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system. Web: https://bitcoin.org/bitcoin.pdf, Son Erişim Tarihi: 20.03.2023.

İnternet: NZ Digital Government (2020). Digital identity trust framework. Web: https://www.digital.govt.nz/digital-government/programmes-and-projects/digital-identity-programme/digital-identity-trust-framework/, Son Erişim Tarihi: 20.03.2023.

İnternet: Otto, N., Lee, S., Sletten, B., Burnett, D., Sporny, M. ve Ebert, K. (2019). Verifiable credentials use cases. Web: https://www.w3.org/TR/vc-use-cases, Son Erişim Tarihi: 20.03.2023.

İnternet: Sporny, M., Longley, D. ve Chadwick, D. (2019). Verifiable credentials data model 1.0. Web: https://www.w3.org/TR/vc-data-model, Son Erişim Tarihi: 20.03.2023.

İnternet: Statista (2022). Global retail e-commerce market size 2014-2023. Web: https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/ Son Erişim Tarihi: 20.03.2023.

İnternet: The Better Identity Coalition. (2019). Better identity in America: A blueprint for policymakers. https://static1.squarespace.com/static/5a7b7a8490bade8a77c07789/

t/5d419caa5001d70001614b8f/1564581036670/Better_Identity_Coalition%2BBlueprint%2B-%2BJuly%2B2018.pdf, Son Erişim Tarihi: 20.03.2023.

İnternet: The International Telecommunication Union (ITU). (2018). Digital identity roadmap guide. http://handle.itu.int/11.1002/pub/81215cb9-en, Son Erişim Tarihi: 20.03.2023.

İnternet: TOBB. (2018). Güven damgası. Web: https://www.guvendamgasi.org.tr/ Son Erişim Tarihi: 20.03.2023.

İnternet: UEKAE. (2015). Elektronik Kimlik Doğrulama Sistemi (EKDS). Web: https://www.ekds.gov.tr/ekds/elektronik-kimlik-dogrulama-sistemi, Son Erişim Tarihi: 20.03.2023.

İnternet: UEKAE. (2015). Kimlik doğrulama yöntemleri. Web: https://www.ekds.gov.tr/ekds/kimlik-dogrulama-yontemleri, Son Erişim Tarihi: 20.03.2023.

İnternet: Usta, A. ve Doğantekin, S. (2019). *Blockchain 101*. Bankalararası Kart Merkezi. https://www.bkm.com.tr/wp-content/uploads/2019/08/15082019_kitap.pdf, Son Erişim Tarihi: 20.03.2023.

İnternet: W3C. (2019, 19 Kasım). Verifiable Credentials Data Model 1.0. Web: https://www.w3.org/TR/vc-data-model/, Son Erişim Tarihi: 20.03.2023.

Jamal, A., Helmi, R. A., Syahirah, A. S. ve Fatima, M. A. (2019). Blockchain-based identity verification system. *2019 IEEE 9th International Conference on System Engineering and Technology (ICSET)*, (s. 253-257).

Jøsang, A., Ismail, R., Boyd, C. (2006). A Survey of Trust and Reputation Systems for Online Service Provision. *Decision Support Systems*, 43, s. 618-644. doi: 10.1016/j.dss.2005.05.019.

Kamvar, S., Schlosser, M. ve Garcia-Molina, H. (2003). The eigentrust algorithm for reputation management in P2P networks. *Proceedings of The 12th International Conference on World Wide Web*, s. 640-651.

Koutrouli, E. ve Tsalgatidou, A. (2012). Taxonomy of attacks and defense mechanisms in P2P reputation systems—Lessons for reputation system designers. *Computer Science Review*, 6, 47-70.

Kugblenu, C. ve Vuorimaa, P. (2020). Decentralized reputation system on a permissioned blockchain for e-commerce reviews. *17th International Conference On Information Technology–New Generations (ITNG 2020)*, s. 177-182.

Li, M., Zhu, L., Zhang, Z., Lal, C., Conti, M. ve Alazab, M. (2021). Anonymous and verifiable reputation system for e-commerce platforms based on blockchain. *IEEE Trans. Netw. Serv. Manage*, 18(4), 4434–4449. doi: 10.1109/TNSM.2021.3098439

Liao, C.-H., Guan, X.-Q., Cheng, J.-H. ve Yuan, S.-M. (2022). Blockchain-based identity management and access control framework for open banking ecosystem. *Future Generation Computer Systems*, 450-466.

Lim, J. (2020). Self-sovereign identity: The harmonising of digital identity solutions through distributed ledger technology. *Australian National University Journal of Law and Technology*, 1(97).

Lim, S. Y., Fotsing, P. T., Almasri, A., Musa, O., Kiah, M. L., Ang, T. F. ve Ismail, R. (2018). Blockchain technology the ıdentity management and authentication service disruptor: A survey. *International Journal on Advanced Science, Engineering and Information Technology,* 8(4), 1735. doi: 10.18517/ijaseit.8.4-2.6838

Liu, J., Hodges, A., Clay, L. ve Monarch, J. (2020). An analysis of digital identity management systems - a two-mapping view. *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, (s. 92-96).

Mendes, G., Chen, D., Silva, B., Serrao, C. ve Casal, J. (2021). A novel reputation system for mobile app stores using blockchain. *Computer*, 54, 39-49.

Nguyen, M., Bai, Q. ve Yu, J. (2020). A Blockchain-based trust model for crowdenvironments. *ACSW 20: Proceedings Of The Australasian Computer Science Week Multiconference*, s. 1-7.

Nitin, N. ve Jenkins, P. (2020). Self-sovereign identity specifications: Govern your ıdentity through your digital wallet using blockchain technology. *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, (s. 90-95).

Omori, R. ve Kishigami, J. (2019). Incorporating reputation system in blockchain-based distributed auctions. *2019 IEEE 8th Global Conference On Consumer Electronics (GCCE)*, s. 1115-1117.

Owiyo, E., Wang, Y., Asamoah, E., Kamenyi, D. ve Obiri, I. (2018). Decentralized privacy preserving reputation system. *2018 IEEE Third International Conference On Data Science In Cyberspace (DSC)*, s. 665-672.

Park, J., Youn, T., Kim, H., Rhee, K. ve Shin, S. (2018). Smart contract-based review system for an IoT data marketplace. *Sensors*, 18(10), 3577. Doi: 10.3390/s18103577

Pöhn, D. ve Hommel, W. (2020). *An overview of limitations and approaches in identity management.* Proceedings of the 15th International Conference on Availability, Reliability and Security' de sunuldu.

Ramachandiran, R. (2018). *Using blockchain technology to improve trust in ecommerce reviews.* College Park, Maryland: Independent Study. doi: 10.13140/RG.2.2. 29324.00646

Rasouli, H., Valmohammadi, C., Azad, N. ve Esfeden, G. A. (2021). Proposing a digital identity management framework: A mixed-method approach. *Concurrency and Computation: Practice and Experience*, 33(17). doi: 10.1002/cpe.6271

Resnick, P. (2002). Trust among strangers in internet transactions: Empirical analysis of eBay's reputation system. *Advances in Applied Microeconomics*, 11, 127-157. doi: 10.1016/S0278-0984(02)11030-3

Schaub, A., Bazin, R., Hasan, O. ve Brunie, L. (2016). A trustless privacy-preserving reputation system. *ICT Systems Security and Privacy Protection*, 398-411.

Soska, K., Kwon, A., Christin, N. ve Devadas, S. (2016). Beaver: A decentralized anonymous marketplace with secure reputation. *IACR Cryptol. EPrint Arch*, 464.

Sun, S., Liu, Y. ve Guo, G. (2019). A privacy-preserving and robust reputation system based on blockchain. *2019 IEEE Intl Conf On Parallel Distributed Processing With Applications, Big Data Cloud Computing, Sustainable Computing Communications, Social Computing Networking (ISPA/BDCloud/SocialCom/SustainCom)*, s. 634-639.

Tamang, S. (2018). *Decentralized reputation model and trust framework blockchain and smart contracts*, Yayımlanmamış Yüksek Lisans Tezi, Uppsala University, Uppsala.

Temoshok, D. ve Abruzzi, C. (2018). *Developing trust frameworks to support identity federations*. Gaithersburg: National Institute of Standards and Technology. doi: 10.6028/NIST.IR.8149

TSE. (2017, 24 Nisan). Elektronik kimlik doğrulama sistemi - Bölüm 1: Genel bakış. Ankara.

Türkiye Cumhuriyeti Kimlik Kartı Elektronik Kimlik Doğrulama Sistemi Yönetmeliği. (2020, 22 Ekim). *Resmi Gazete*.

Vandervort, D. (2014). Challenges and opportunities associated with a bitcoin-based transaction rating system. *Financial Cryptography and Data Security*, 33-42.

Wang, K., Zhang, Z. ve Kim, H. (2018). ReviewChain: Smart contract based review system with multi-blockchain gateway. *2018 IEEE International Conference On Internet Of Things (iThings) And IEEE Green Computing And Communications (GreenCom) And IEEE Cyber, Physical And Social Computing (CPSCom) And IEEE Smart Data (SmartData)*. s. 1521-1526.

Yang X. vd. (2020). LedgerDB: A centralized ledger database for universal audit and verification. *Proc. VLDB Endow*, 13(12), 3138–3151. doi: 10.14778/3415478.3415540

Yang, X. vd. (2022). Ubiquitous verification in centralized ledger database. *2022 IEEE 38th International Conference on Data Engineering (ICDE)*, Kuala Lumpur, Malaysia, s. 1808–1821. doi:10.1109/ICDE53745.2022.00181

Zulfiqar, M., Tariq, F., Janjua, M., Mian, A., Qayyum, A., Qadir, J., Sher, F. ve Hassan, M. (2021). EthReview: An ethereum-based product review system for mitigating rating frauds. *Computers – Security*, 100, 102094.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı	: DOĞAN, Ömer
Uyruğu	: T.C.
Doğum tarihi ve yeri	: -
Medeni hali	: -
Telefon	: -
e-mail	: -

Eğitim

Derece	**Eğitim Birimi**	**Mezuniyet Tarihi**
Doktora	Gazi Üniversitesi / Bilişim Enstitüsü	Devam ediyor
Yüksek lisans	ODTÜ / Enformatik Enstitüsü	2015
Lisans	ODTÜ / Elektrik Elektronik Mühendisliği	2003
Lise	Denizli Anadolu Lisesi	1998

İş Deneyimi

Yıl	**Yer**	**Görev**
2010-Halen	STM Savunma Teknolojileri	Başmühendis
2009-2010	Innova A.Ş.	Yazılım Mühendisi
2001-2008	BYDS Ltd. Şti.	Yazılım Mühendisi

Yabancı Dil

İngilizce

Yayınlar

1. Ömer Doğan, Hacer Karacan, "A Blockchain-based E-Commerce Reputation System Built with Verifiable Credentials" in IEEE Access vol.11, pp.47080-47097, 2023 (SCI-Expanded), DOI: 10.1109/ACCESS.2023.3274707
2. Ömer Doğan, Hacer Karacan, "Türkiye'deki e-Ticarete Özgü Blokzincir Tabanlı

Dijital Kimlik Güven Çerçevesi Önerisi", Bilgi Yönetimi cilt.5, sa.2, ss.256-279, 2022 (Hakemli Dergi), DOI: 10.33721/by.1113558



GAZİLİ OLMAK AYRICALIKTIR.