Discover Education

Discover

Perspective

Holochain: a novel technology without scalability bottlenecks of blockchain for secure data exchange in health professions education

Yavuz Selim Kıyak[1] · Alex Poor[2,3] · Işıl İrem Budakoğlu[1] · Özlem Coşkun[1]

Received: 25 May 2022 / Accepted: 12 September 2022
Published online: 15 September 2022
© The Author(s) 2022 OPEN

Abstract
The efficacy of health professions education (HPE) is more and more reliant on leveraging new technologies as they emerge. The nascent "Web 3.0" is shifting us away from traditional centralized architectures for capture and storage of information, and aims to decentralize and distribute it. Blockchain has received a large amount of attention as a promising "Web 3.0" technology and has been applied in the HPE setting. In this paper we argue that blockchain has two core issues which have prevented its widespread adoption: scalability and environmental impact. The architecture of blockchain means that all participating nodes must store and validate all of the data. This creates a large amount of overhead, which does not scale well. Similarly, there is growing awareness that the energy requirements of validating blockchain transactions run counter to global efforts to mitigate climate change. Holochain, however, is a novel Web 3.0 technology that aims to overcome both of these issues. Its architecture is fundamentally different to blockchain, by virtue of being "agent-centric" rather than "data-centric". That is, each piece of data does not need to be globally validated—and yet Holochain can still guarantee data validity and integrity. We identify that specific challenges in the HPE setting—tracking educational activities, accountable mechanisms for observing entrustable professional activities, and validation of third-party certification and credentialing—can all be achieved elegantly in Holochain, without experiencing any of the disadvantages evidenced in blockchain.

Keywords Holochain · Blockchain · Scalability · Distributed ledger technologies · Health professions education

1 Introduction

Health professions education (HPE) needs to adapt as technology evolves. We have witnessed that the adoption of advances in technology such as e-learning [1], online assessment [2], technology-enhanced learning [3], artificial intelligence and deep learning [4]—have all permeated into HPE. However, the dominant architectural model has been one of centralization—where the data is managed and stored by third parties who must take responsibility for maintaining data integrity, data security and validation. There have been high-profile issues with this model [5], which has led to the development of "Web 3.0" [6] which prioritizes decentralized and distributed approaches.

Blockchain offered an interesting solution to overcome these problems, using distributed ledger technology and cryptography in a data-centric way [7]. It has created opportunities for policymakers in various areas—from banking

✉ Yavuz Selim Kıyak, yskiyak@gazi.edu.tr | [1]Medical Education and Informatics, Gazi University Faculty of Medicine, Gazi Üniversitesi Hastanesi E Blok 9. Kat, 06500 Beşevler, Ankara, Turkey. [2]Auckland University of Technology, Auckland, New Zealand. [3]Pinnacle Midlands Health Network, Hamilton, New Zealand.

and finance, to healthcare and education [8]. In spite of the advantages, it suffered from a scalability problem that requires users to pay high fees and to wait for hours for the approval of transactions [9]. These bottlenecks have limited its widespread adoption. Bitcoin is perhaps the most well-known blockchain application and, considering environmental impact, it has been estimated that the processing power required to maintain it would cause a 2 °C increase in global temperatures over the next 30 years [10]. Although innovators in the field have attempted to find ways to overcome these bottlenecks to make blockchain more efficient [9], its data-centric structure has stymied meaningful progress.

Holochain, by contrast, represents a paradigm shift by offering instead an agent-centric approach. We contend that it holds a lot of promise for maintaining data integrity and security in networks, whilst responding to the two core problem areas for blockchain—scalability and environmental impact [11, 12]. Whilst its potential seems very exciting, we should bear in mind that Holochain is not yet being used in production environments at the time of writing; the research community has had more time with blockchain to identify issues. Nevertheless, we will show that it has real potential in the HPE setting.

Blockchain technology has been evaluated in the HPE literature before [13], however the problems of scalability and environmental impact were not addressed. We contend that Holochain's agent-centric approach has the potential to solve both issues, and this is something that currently has no base in the HPE literature. Our aims in this article, therefore, are to (a) provide an overview of blockchain technology and identify the bottlenecks, (b) provide an overview of Holochain and explain both the agent-centric approach and how it might solve the scalability problem, and (c) identify some issues specific to HPE and compare how they may be resolved by the different approaches of both technologies.

2 Blockchain technology and its bottlenecks

Blockchain offers a cryptographically secured and decentralized data exchange using distributed ledger technology that employs a novel data management model [14]. The data is stored in blocks that are chained together in chronological order. The process of recording the data into blocks depends on the miners instead of centralized third-party actors such as financial institutions, notaries, etc. A user attempts to record the data in the chain, for example sending one Bitcoin, and then the miners approve the transaction if it is valid. The miners reach a consensus on validation, then broadcast the data to the nodes who hold the full ledger including all previous transaction. Once stored within the blockchain, data is immutable [14]. Subsequently, the next block of data goes through the same process.

To describe it more simply, there is a publicly transparent ledger that contains every single transaction. Before blockchain emerged, these records would have been stored in a centralized way—under the control of a single entity. But now thousands of people all around the world can hold the same up-to-date copy of the ledger by way of blockchain [15]. The miners are the only actors who can add a block to the immutable chain by reaching a consensus [15]. By doing so, the need for centralized bodies as intermediaries for data validation is replaced with collective control [7].

Blockchain has moved us away from the vulnerabilities of centralization. If you hold the data in a centralized server—where it can only be changed by authorized officials—your data (and these officials) are very attractive targets for hackers. Because all power is concentrated in the center, there are a very small number of potential access points to change the data. Blockchain, however, distributes the same cryptographically secured copies all around the world immutably, and the copies can only be extended through reaching consensus by thousands of miners who earn incentives due to their work [15]. Therefore, it is nearly impossible to hack.

In spite of its advantages, some serious challenges stand in the way of widespread blockchain adoption. The two most prominent of these challenges are scalability (low amount of data exchange with low speed and high cost), and the negative environmental effects of blockchain's energy requirements [16].

For instance, Bitcoin can process only seven transactions per second, and the size of the blocks produced every 10 min is only one megabyte [17]. If you consider the huge amount of data exchange generated globally every second, it becomes evident that blockchain cannot handle large amounts of traffic. If you increase the block size, the amount of data that miners have to store gets higher. In turn, the requirements to procure new hardware to store this data, and the costs associated with it, will lead to miners deciding to quit. The net result is fewer miners and a less decentralized network. This represents a serious threat to the security of the network. This tradeoff between decentralization, scalability, and security is referred to as the "blockchain trilemma" [16]. Apart from the scalability problem, the amount of energy that is consumed by blockchains is enormous. Although humanity is currently dealing with the threat of climate change, the Bitcoin blockchain alone already consumes more energy than Argentina or Netherlands as of 2021 [18].

In conclusion, blockchain is an important improvement for data exchange without relying on centralized intermediaries. However, its bottlenecks stand in the way of more widespread adoption. The root of these serious problems is the data-centric view embedded in blockchain technology. In order to overcome it, "thinking outside the blocks" would be helpful, and this is where Holochain's agent-centric technique offers an interesting alternative.

3 Holochain's agent-centric technology

Holochain is an open-source application development framework [11]. It can be described as a peer-to-peer networking protocol that enables us to develop truly serverless applications [19]. Each user runs Holochain applications (hApps) on their own device. Contrary to blockchain, hApps predominantly host only that user's data, and there is no requirement to store or validate all network data. It is a combination of BitTorrent, Git, and cryptographic signatures [20]. Security is maintained through cryptography and peer accountability [19].

Holochain is inspired by nature [19]. While blockchain nodes hold all of the data generated by all users, nodes in Holochain hold only their own data and a "shard" of other network data, always acting in accordance with their "DNA" which is a set of immutable rules that are determined by the creator of the hApp [21]. Following this biological metaphor, blockchain can be thought of as a system where human cells have to receive and hold all the data of every single other cell in real-time, before every transaction [19]. It is incompatible with life. However, the cells in nature work through only using their own information combined with the cells that they interact with. Due to this nature-inspired point of view, Holochain employs an agent-centric model rather than blockchain's data-centric model that requires global consensus [12]. In Holochain, the primary system component is users, not servers or data. A comparison of the differing architectures, based on the pioneering work of Paul Baran back in 1964 [22], is revealed in Fig. 1. It shows firstly (from left to right) the dominant centralized model. Secondly, the decentralized architecture is a prescient representation of blockchain, where each node contains a copy of all the data and clients connect to those nodes. Finally, a fully distributed network is shown where peers connect directly to other peers and, collectively, have access to all the data within the network. This is an accurate representation of how Holochain operates.

Holochain describes itself using four steps [20]:

> "You install an app, which signs and stores your data on your device. You share your public data with a random set of peers. Your peers validate the data against the app's rules before storing it. Invalid data triggers a network-wide security response."

Each agent stores its own data and runs its own copy of the code contrary to blockchains' global monolithic ledger [23]. The network allows applications to run according to the rules determined by the creator and participants of the hApp. This set of rules determines how the users can interact with each other. To ensure the rules—no matter what has been determined by the users—are not violated, two pillars of Holochain step in: Intrinsic data validity and peer witnessing [19].

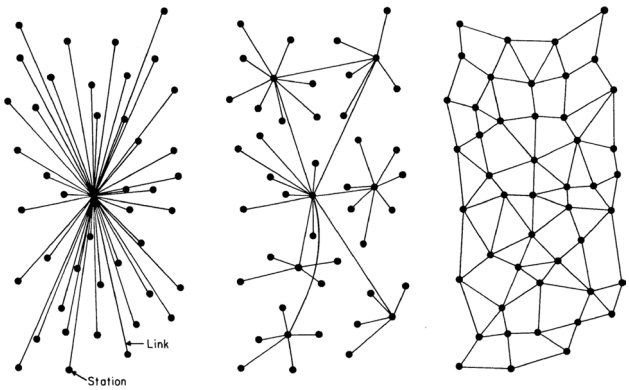


Fig. 1 Architecture comparison; centralized, decentralized, and distributed, respectively from the left to the right

To sustain intrinsic data validity, Holochain employs cryptography to prove authorship and detect tampering. All actions committed by an agent are recorded on its own chain immediately after the agent signs it using the private key. Any third-party agent is not able to interfere with it. However, it is still possible for each agent to tamper with its own data, due to the fact that every agent has the right to do anything with their own data that they store on their chain. Peer witnessing fills this gap. Each piece of public data on the network is validated and stored by a random set of peers. If these random peers detect any malicious behavior or identify that any rules of the game have been broken, they gossip with other peers to identify and isolate the corrupt actor [21]. These two pillars create a robust mechanism that Holochain describes as "a multicellular social organism with a memory and an immune system. It mimics the way that biological systems have managed to thrive in the face of novel threats for millions of years" [19].

In short, Holochain acts as an "unenclosable carrier" [24], "to create a network of individuals, interacting freely with each other, playing by a shared set of rules" [19]. The ultimate result of this agent-centric approach is an advantageous framework that enables developers to create serverless apps that are impossible to hack since each user participates in the network infrastructure by supplying their own storage and takes responsibility for data validation, distinct from centralized solutions [25]. This can all take place on a user's own device, or a Holo device that consumes as much electricity as a standard light bulb [26] so it can be considered as "green technology". In other words, it enables us to exchange data without blockchain's bottlenecks. While blockchain, for example the Ethereum network, necessitates paying dozens, sometimes thousands, of dollars and waiting minutes or hours for each transaction [27], it has been demonstrated that Holochain is able to do all of that (and more) instantly and with significantly lower costs [28]. In conclusion, as we pointed out in our previous study [29], Holochain has enormous potential to open a new age by making the as-yet-unrealized dreams of blockchain come true.

4 Blockchain vs Holochain in HPE

Cybersecurity has a critical role in the sustainability of academic health centers. Cyberattacks have a catastrophic effect on highly centralized health systems, including education that is carried out in these centers. Millard [30] notes a malware incident that resulted in the loss of IT (information technology) systems for 45 days at an academic health center. More recent examples include a ransomware attack on Ireland's national health system, leaving systems non-operational for up to 4 months [31], and a ransomware attack on a major New Zealand hospital system that disrupted IT systems and hospital services for more than 1 month [32]. It affects not only healthcare services but also HPE processes and activities. To prevent these types of problems, it was necessary to develop educational programs to improve cybersecurity awareness [33].

Holochain, however, has the potential to address the root cause of this problem—rather than merely the symptoms. As we have already noted, a highly centralized architecture means that gaining access to even one part of a network or system potentially gives you the ability to unlawfully access or tamper with the whole of an organization's data. In the blockchain model, the ledger may already be publicly available and so security threats tend to center on gaining control over a majority of nodes (a "51% attack"). There is evidence in the literature of data integrity in blockchain networks being compromised in scenarios where less than 51% is controlled [34]. Both paradigms offer the potential that all data can be unlawfully accessed, or the entire network itself can be compromised [35, 36].

Holochain makes this kind of attack pattern impossible by design. Even if a bad actor were able to defeat the cryptographic protection of one user's device, then only that user's data—and the "shard" of data distributed to it by other users—would be compromised. When the documentation about distributed hash tables in Holochain is considered [19], it would be concluded that to access, or tamper with, the *entire* network data set is all but impossible. Furthermore, bad actors are prevented from expanding their reach into the network by the "intrinsic data validity" and "peer witnessing" functions we have already discussed. There is almost no peer-reviewed literature on Holochain security, although Frahat et al. [23] indirectly note that Holochain peers independently "sandbox" their data from one another, whereas blockchain peers all hold an identical copy of the network data. This architectural difference is at the heart of the claim that any Holochain network compromise would be very limited; compromising a single blockchain peer would provide access to all the network data (something that would only be of interest if the network was already permissioned and not publicly accessible), whereas compromising a single Holochain peer would provide access to that user's data plus a portion of sharded network data. If we are discussing a compromise that would provide *control* of a network, this concept simply has no relevance in Holochain. Controlling an Ethereum network (for example, via a 51% attack) would allow the attacker to direct currency to their wallet, thus realizing a tangible economic gain (insofar as the token is tangible). This

notion of "control" is particular to blockchain because of its cumbersome consensus and validation process; there is no equivalent in Holochain and thus, unless a developer has specifically designed a hApp which provides that functionality, it is not possible by default for an attacker to meaningfully influence a Holochain network without compromising each individual peer [19].

Notwithstanding this, it is true that Holochain has not yet been studied or tested anywhere near as extensively as blockchains, and there may be as yet unforeseen security issues which can only be found when used at scale. Nevertheless, we draw attention here to a fundamental difference in architecture which appears to support cybersecurity risk mitigation.

As we have seen in examples from Ireland and New Zealand (but there are many others), the practical impact of a cybersecurity incident is a disruption to IT system availability. Specifically, in both these examples, access to electronic information was simply not possible. Not only does this pose an unacceptable risk to patient care, but it is also a serious impediment to the efficacy and sustainability of HPE activities. Holochain offers another solution to this problem via the way it distributes data across users or nodes. If one, or even several nodes, were compromised by bad actors and they were not able to serve data to other network users, there would be no loss of access to data overall. Enough data would still be shared randomly across other nodes, to make sure it is always available if required.

The problem is not restricted to preventing cyberattacks. HPE has more specific challenges such as the difficulty of tracking educational activities, providing an accountable mechanism for the observation of entrustable professional activities (EPAs), and trusting third-party intermediaries for certification and credentialing. Funk et al. [13] suggest that HPE can be built on a blockchain-based system to overcome these challenges. However, the real life implementation was questioned because of concerns about blockchain being expensive, slow, and needing to consume substantial amounts of energy [37].

For instance, a decentralized credentialing system for continuing medical education (CME) was developed using the Ethereum blockchain [38]. According to Statista, the average gas fee on the Ethereum network was between US$ 32 and US$ 210 in 2021 [39]. It means that, any new data related to the credentialing status of a doctor—for example participating in a CME activity—would have cost at least US$ 32 to validate. Even if these transaction costs were acceptable, Bitcoin is notable for being able to process only seven transactions per second [40] and both consuming a disproportionately large amount of electricity and generating relatively large amount of CO^2 [41]. Blockchain's ability to effectively *scale* to real world applications is therefore debatable.

Furthermore, a recent literature review [42] showed that blockchain's data-centric approach has many inherent challenges in terms of compliance with the General Data Protection Regulation (GDPR), (the prevailing European Union (EU) law that regulates data protection and privacy for EU citizens, which has also served as a model for regulatory reform in many other jurisdictions [43]). For instance, blockchain's data immutability contradicts directly with the so-called "right to be forgotten" (GDPR Article 17). Wahlstrom et al. [25] focus on this disparity and identify Holochain as a technology that offers better regulatory compliance due to its "soft" immutability. That is to say, Holochain permits data to be updated, modified or even removed according to the rules defined in the hApp but, similarly, it is also possible to enforce real immutability if required.

Tracking educational activities through e-portfolios without relying on centralized servers may be possible with Holochain. E-portfolios should provide a personal space for the students to store their educational activities, patient cases, and reflections on their learning process [44]. Due to this reason, a portfolio could contain private or sensitive content that requires a restriction mechanism that allows the students or supervisors to determine who can access it [1]. We have already seen that centralized solutions are vulnerable, but we should also consider that storing the data with the help of a corporation's cloud services poses a serious threat to privacy [45]. In a centralized model, it can be very hard for users to know who has accessed their data without consent.

In HPE, the importance of security, privacy, and integrity of data is not only for e-portfolios. The literature pointed out the importance in terms of a wide range of areas within HPE such as digital learning environments [46], learning analytics [47], artificial intelligence [48], ethics and scholarship [49], and even student wellbeing [50]. Although blockchain technology could offer decentralized solutions to the problems in these areas, its scalability issues represent meaningful barriers, which are not experienced in Holochain.

Whilst we have identified that the agent-centric approach of Holochain has many advantages over blockchain's data-centric view, it is certainly not without issues of its own. As of July 2022, the primary issue is that Holochain has not even had a 'beta' version release, meaning that all current development comes with important caveats around its readiness for production usage. Because of this, Holochain has not yet been tested in earnest in any real life environment. Whilst we want to draw the research community's attention to its exciting possibilities and important architectural differences, it

is true that we simply do not yet know how it would actually perform at scale. Given its identified advantages, however, we hope that future research develops hApps for use in HPE in order to evaluate whether implementation is feasible, and to provide a more evidence-based comparison with blockchains and centralized solutions. Moreover, a research on a comparison of centralized solutions, blockchains, and Holochain in terms of carbon footprints would be valuable. It may compare the impact of these different approaches on climate change when they are used in health professions education.

5 Conclusion

There are well-established issues with the dominant centralized model of architecting technology solutions; we have identified vulnerability to hacking and ransomware as an example. Web 3.0 technologies are maturing, and offer us the possibility to move away from this paradigm. These have huge potential within HPE.

To date, blockchain has been the focus of scholarly work in this area. However, we identify critical issues with the practical application of blockchain in HPE. Holochain is a novel framework that overcomes the limitations of blockchain and allows us to realise the potential of Web 3.0 without blockchain's limitations.

Holochain is a secure peer-to-peer networking framework, which allows the development of hApps and the implementation of networks (for example, e-portfolios) that are completely decentralized yet can still guarantee privacy, security, and data integrity. E-portfolios are currently highly centralized, and particularly vulnerable to hacking or exploitation by a bad actor. Holochain similarly can offer benefits in many other domains of HPE such as digital learning environments, learning analytics systems, and artificial intelligence.

While blockchain's scalability issues have prevented widespread adoption, Holochain can provide a framework for decentralized and scalable apps upon which any school could build its HPE curriculum. This furthermore means that Holochain has the potential to effect radical changes in HPE.

This research raises questions about the Web 3.0 future of HPE and suggests that further research into practical HPE applications of Holochain will highlight its full potential.

Author contributions Conceptualization: YSK, İİB; Writing—original draft: YSK, AP, İİB, ÖC; Writing—review and editing: YSK, AP, İİB, ÖC; Supervision: ÖC. All authors read and approved the final manuscript.

Funding This research did not receive any specific grant.

Data availability Not applicable.

Code availability Not applicable.

Declarations

Competing interests The authors declare that they have no conflict of interest.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. Ellaway R, Masters K. AMEE Guide 32: e-Learning in medical education Part 1: learning, teaching and assessment. Med Teach. 2008;30(5):455–73.
2. Dennick R, Wilkinson S, Purcell N. Online eAssessment: AMEE guide no. 39. Med Teach. 2009;31(3):192–206.
3. Cook DA, Ellaway RH. Evaluating technology-enhanced learning: a comprehensive framework. Med Teach. 2015;37(10):961–70.
4. Lee J, Wu AS, Li D, Kulasegaram K. Artificial intelligence in undergraduate medical education: a scoping review. Acad Med. 2021;96(11S):S62-70.
5. Golbeck J, Aral S. Why the Cambridge analytica scandal ıs a watershed moment for social media. Knowledge at Wharton. 2018. https://knowledge.wharton.upenn.edu/article/fallout-cambridge-analytica/. Accessed 7 Apr 2022.
6. Rudman R, Bruwer R. Defining Web 3.0: opportunities and challenges. EL. 2016;34(1):132–54.

7. Yli-Huumo J, Ko D, Choi S, Park S, Smolander K. Where is current research on blockchain technology?—a systematic review. PLoS ONE. 2016;11(10):e0163477.
8. Kara O, Kurutkan MN. Applications of blockchain technologies in health services: a general framework for policymakers. In: Kahyaoğlu SB, editor. The ımpact of artificial ıntelligence on governance, economics and finance, vol. I. Berlin: Springer; 2021. p. 201–32.
9. Xie J, Yu FR, Huang T, Xie R, Liu J, Liu Y. A survey on the scalability of blockchain systems. IEEE Netw. 2019;33(5):166–73.
10. Mora C, Rollins RL, Taladay K, Kantar MB, Chock MK, Shimada M, et al. Bitcoin emissions alone could push global warming above 2°C. Nat Clim Change. 2018;8(11):931–3.
11. Harris-Braun E, Luck N, Brock A. Holochain-scalable agent centric distributed computing. 2018. https://github.com/holochain/holochain-proto/blob/a0ad5b4a2c5aac257703dc5fba8cab0d2e4660d2/holochain.pdf. Accessed 12 Aug 2021.
12. Manski S. Distributed ledger technologies, value accounting, and the self sovereign identity. Front Blockchain. 2020;3:29.
13. Funk E, Riddell J, Ankel F, Cabrera D. Blockchain technology: a data framework to improve validity, trust, and accountability of information exchange in health professions education. Acad Med. 2018;93(12):1791–4.
14. Niranjanamurthy M, Nithya BN, Jagannatha S. Analysis of Blockchain technology: pros, cons and SWOT. Clust Comput. 2019;22(S6):14743–57.
15. Agbo C, Mahmoud Q, Eklund J. Blockchain technology in healthcare: a systematic review. Healthcare. 2019;7(2):56.
16. Zhou Q, Huang H, Zheng Z, Bian J. Solutions to scalability of blockchain: a survey. IEEE Access. 2020;8:16440–55.
17. Zheng Z, Xie S, Dai H, Chen X, Wang H. An overview of blockchain technology: architecture, consensus, and future trends. In: 2017 IEEE international congress on big data (BigData congress). IEEE; 2017. p. 557–64.
18. Criddle C. Bitcoin consumes "more electricity than Argentina." BBC News. 2021. https://www.bbc.com/news/technology-56012952. Accessed 7 Apr 2022.
19. Holochain Core Concepts. 2021. https://developer.holochain.org/concepts/. Accessed 7 Apr 2022.
20. Holochain. Holochain | App framework with P2P networking. 2021. https://holochain.org. Accessed 7 Apr 2022.
21. Zia MF, Benbouzid M, Elbouchikhi E, Muyeen SM, Techato K, Guerrero JM. Microgrid transactive energy: review, architectures, distributed ledger technologies, and market analysis. IEEE Access. 2020;8:19410–32.
22. Baran P. On distributed communications: I. Introduction to distributed communications networks. 1964. https://www.rand.org/content/dam/rand/pubs/research_memoranda/2006/RM3420.pdf. Accessed 7 Apr 2022.
23. Frahat RT, Monowar MM, Buhari SM. Secure and scalable trust management model for IoT P2P network. In: 2019 2nd ınternational conference on computer applications & ınformation security (ICCAIS). IEEE; 2019. p. 1–6.
24. Brock A, Zemel J. Unenclosable carriers and the future of communication. Holochain. 2020. https://medium.com/holochain/unenclosable-carriers-and-the-future-of-communication-4ac6045ac894. Accessed 7 Apr 2022.
25. Wahlstrom K, Ul-haq A, Burmeister O. Privacy by design: a Holochain exploration. AJIS. 2020;24.
26. Holo. Will Holo use lots of electricity? How much electricity will my HoloPort use?. Holo Support. 2019. https://help.holo.host/support/solutions/articles/36000035595-will-holo-use-lots-of-electricity-how-much-electricity-will-my-holoport-use. Accessed 7 Apr 2022.
27. Binder M. Bored Ape Yacht Club caused Ethereum fees to soar to astronomical levels. Mashable. 2022. https://mashable.com/article/ethereum-gas-fees-skyrocket-bored-ape-yacht-club-otherside-nft-launch. Accessed 17 July 2022.
28. Janjua K, Shah MA, Almogren A, Khattak HA, Maple C, Din IU. Proactive forensics in IoT: privacy-aware log-preservation architecture in fog-enabled-cloud using holochain and containerization technologies. Electronics. 2020;9(7):1172.
29. Kıyak YS, Coşkun Ö, Budakoğlu İ. Blokzinciri, Akıllı Kontratlar Ve Sağlık Alanındaki Üç Uygulama Örneği [Blockchain, Smart Contracts, and Three Implication Examples in Healthcare]. Hacettepe Sağlık İdaresi Dergisi. 2019;22(2):457–66.
30. Millard WB. Where bits and bytes meet flesh and blood. Ann Emerg Med. 2017;70(3):A17-21.
31. McNamee MS. HSE cyber-attack: Irish health service still recovering months after hack. BBC News. 2021 Sep 5. https://www.bbc.com/news/world-europe-58413448. Accessed 7 Apr 2022.
32. Gunasegaran T. "A long way still to go", says Waikato DHB. Healthcare IT News. 2021. https://www.healthcareitnews.com/news/anz/long-way-still-go-says-waikato-dhb. Accessed 7 Apr 2022.
33. Maggio LA, Dameff C, Kanter SL, Woods B, Tully J. Cybersecurity challenges and the academic health center: an interactive tabletop simulation for executives. Acad Med. 2021;96(6):850–3.
34. Sayeed S, Marco-Gisbert H. Assessing blockchain consensus and security mechanisms against the 51% attack. Appl Sci. 2019;9(9):1788.
35. Eyal I, Sirer EG. Majority ıs not enough: bitcoin mining ıs vulnerable. In: Christin N, Safavi-Naini R, editors. Financial cryptography and data security, vol. 8437. Lecture Notes in Computer Science. Berlin: Springer; 2014. p. 436–54.
36. Nayak K, Kumar S, Miller A, Shi E. Stubborn mining: generalizing selfish mining and combining with an eclipse attack. In: 2016 IEEE European symposium on security and privacy (EuroS&P). Saarbrucken: IEEE; 2016. p. 305–20.
37. Walsh K. Could blockchain be applied to healthcare professional education?. The BMJ. 2019. https://blogs.bmj.com/bmj/2019/04/25/kieran-walsh-could-blockchain-be-applied-to-healthcare-professional-education/. Accessed 7 Apr 2022.
38. Rathod J, Gupta A, Patel D. Using blockchain technology for continuing medical education credits system. In: 2020 seventh ınternational conference on Software Defined Systems (SDS). Paris: IEEE; 2020. p. 214–9.
39. Ethereum gas price 2015–2022. Statista. https://www.statista.com/statistics/1221821/gas-price-ethereum/. Accessed 17 July 2022.
40. Zheng Z, Xie S, Dai HN, Chen X, Wang H. Blockchain challenges and opportunities: a survey. IJWGS. 2018;14(4):352.
41. Badea L, Mungiu-Pupazan MC. The economic and environmental impact of bitcoin. IEEE Access. 2021;9:48091–104.
42. Haque AB, Islam AKMN, Hyrynsalmi S, Naqvi B, Smolander K. GDPR Compliant blockchains—a systematic literature review. IEEE Access. 2021;9:50593–606.
43. Breitbarth P. The impact of GDPR one year on. Netw Secur. 2019;2019(7):11–3.
44. Moores A, Parks M. Twelve tips for introducing E-Portfolios with undergraduate students. Med Teach. 2010;32(1):46–9.
45. Doctorow C. With great power comes great responsibility: platforms want to be utilities, self-govern like empires. Electronic Frontier Foundation. 2021. https://www.eff.org/deeplinks/2021/08/utilities-governed-empires. Accessed 7 Apr 2022.
46. Thoma B, Turnquist A, Zaver F, Hall AK, Chan TM. Communication, learning and assessment: exploring the dimensions of the digital learning environment. Med Teach. 2019;41(4):385–90.

47. ten Cate O, Dahdal S, Lambert T, Neubauer F, Pless A, Pohlmann PF, et al. Ten caveats of learning analytics in health professions education: a consumer's perspective. Med Teach. 2020;42(6):673–8.
48. Webster CS. Artificial intelligence and the adoption of new technology in medical education. Med Educ. 2021;55(1):6–7.
49. Masters K. Ethics in medical education digital scholarship: AMEE Guide No. 134. Med Teach. 2020;42(3):252–65.
50. Gengoux GW, Roberts LW. Ethical use of student profiles to predict and prevent development of depression symptoms during medical school. Acad Med. 2019;94(2):162–5.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.