SECURITY IN THE BLOCKCHAIN IN HEALTH CARE SECTOR

BIZTONSÁG A BLOKKLÁNCBAN AZ EGÉSZSÉGÜGYI SZEKTORBAN

QOSE, Silvana[1]

Abstract

With the advent of Health 4.0, the healthcare industry is entering a new age of innovation. Through data-based learning and system interconnectivity, the integration of cutting-edge technologies such as cyber-physical systems (CPS), big data, cloud computing, machine learning, and blockchain with healthcare services has enhanced performance and efficiency. One of the significant difficulties facing the healthcare business is protecting sensitive data from cyberattacks while maintaining privacy through verified access. For this reason, implementing blockchain-based networks can significantly reduce healthcare systems' vulnerabilities and safeguard their data. In order to better understand how blockchains might be used to safeguard healthcare data, this article addresses the following questions: what data are used, when do we need them, why do we need them, and who needs them? We identify and explore the technological constraints and legal issues related to blockchain-based healthcare data security deployment to give a roadmap for future research areas we can conduct or instruct.

Keywords

blockchain technology, cyber-physical systems (CPS), healthcare systems, data security, authentication, trusted data sharing

Absztrakt

Az Egészség 4.0 megjelenésével az egészségügyi ágazat az innováció új korszakába lép. Az adatalapú tanulás és a rendszerek összekapcsolhatósága révén az élvonalbeli technológiák, például a kiber-fizikai rendszerek, a big data, a felső alapú számítástechnika, a gépi tanulás és a blockchain integrálása egészségügyi szolgáltatásokkal javította a teljesítményt és a hatékonyságot. Az egészségügyi üzletág egyik jelentős nehézsége az érzékeny adatok védelme a kibertámadásokkal szemben, miközben ellenőrzött hozzáférés révén megőrzi a magánélet védelmét. Emiatt a blokklánc-alapú hálózatok bevezetése jelentősen csökkentheti az egészségügyi rendszerek sebezhetőségét és megóvhatja adataikat. Annak érdekében, hogy jobban megértsük, hogyan használhatók a blokkláncok az egészségügyi adatok védelmére, ez a cikk a következő kérdésekkel foglalkozik: milyen adatokat használunk, mikor van szükségünk rájuk, miért van szükségünk rájuk és kinek van szüksége rájuk? Azonosítjuk és feltárjuk a technológiai korlátokat és jogi problémákat, amelyek a blokklánc alapú egészségügyi adatbiztonság kiépítéséhez kapcsolódnak, hogy ütemtervet adhassunk a jövőbeli kutatási területekhez, amelyeket végezhetünk vagy utasíthatunk.

Kulcsszavak

blockchain technológia, kiberfizikai rendszerek (CPS), egészségügyi rendszerek, adatbiztonság, hitelesítés, megbízható adatmegosztás

[1] qose.silvana@phd.uni-obuda.hu | ORCID: 0000-0002-8946-5722 | PHD student, Óbuda University Doctoral School for Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

INTRODUCTION

Each medical facility uses a different data storage technology and protocol, and each has its strict policies governing the exchange and transfer of patient data. The current data collection method cannot guarantee the integrity and liability of patients' medical records.

Classical healthcare systems have several challenges, including storing patient data and safely moving it throughout healthcare information networks. All participants and stakeholders may quickly and securely integrate healthcare data using a distributed blockchain platform. One of the issues facing the medical community is safeguarding patient data while making it accessible whenever necessary. This issue can be resolved, and data may be shared safely and unaltered thanks to blockchain technology has distributed and irreversible nature.

Integrating blockchain technology into medical healthcare systems may resolve the issues mentioned earlier via various encryption techniques, consensus processes, and peer-to-peer networks.

Blockchain is technically described as a distributed, decentralized, peer-to-peer database network that enables any number of participants – including those we cannot trust – to conduct transactions without outside intervention and is used to maintain data integrity. It is a distributed ledger that performs transactions and creates informational records that can be verified and kept for all time. Three fundamental ideas – peer-to-peer networks, public key cryptography, and distributed consensus – become the foundation of blockchain technology and transactions.

WHAT IS A BLOCK IN A BLOCKCHAIN?

The transaction data information is contained in the block, which is a record and includes the following information [1].

1. The block's alphanumeric number is hashed for identification.
2. The block's previous block's hash.
3. Time mine
4. A single random integer is utilized to change the hash value.
5. In a blockchain network, a Merkle root is the hash of all the transactions that make up a block.
6. Transaction data that includes information on many transactions.

A. What Blockchain characteristics include [2], [3]:

The fact that Blockchain is a peer-to-peer network and anybody can join without changing the data is one of its core characteristics. Time mining is used to demonstrate the presence of records inside a specific time frame, and it may also be helpful to spot any unauthorized changes. As a result of data being immutable after it has been written to a blockchain, it is called immutable.

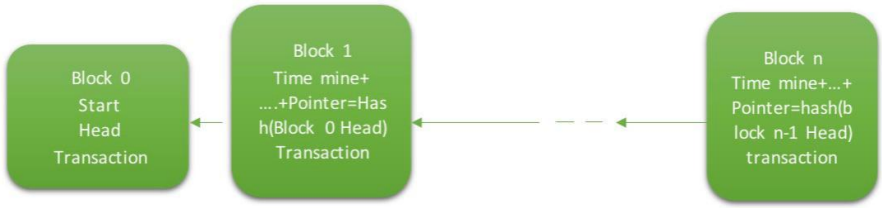

Fig. 1 Blocks from 0 to n (self edition)

There is no network breakdown due to blockchain technology's dispersed, decentralized nature. Because creating a revocation method is complicated and the Blockchain is a public resource, complexity puts costs on other users, making the Blockchain irreversible by the sender. Due to all of the features of blockchain technology, it is crucial to protect patient medical information and transfer them securely as needed.

B. What is Hash Rate, and why is it important to understand it in order to assess the chain's security?

The hash rate measures the computing power of a proof-of-work (PoW) cryptocurrency network [4]. A blockchain network's health, security, and mining difficulty are assessed using its mining power.

A hash is a randomly produced alphanumeric code and guessing it is known as hashing (or as close to it as possible). The number of guesses made by computers on the network is counted, and the hash rate indicates how many guesses are made per second over the whole network.

B.1. Key lesson

The hash rate gauges the processing power on a blockchain network.

How many assumptions are made per second that affect the hash rate?

A blockchain network's security and mining difficulty may be estimated using its average hash rate.

Hash rates can fluctuate over time, with the most widely used blockchains seeing an annual increase.

The amount of tries each computer performs per second to solve the hash on a blockchain network is used to measure hash rates. This is a crucial step in the proof-of-work (PoW) network's crypto-mining process.

B.2. How it works:

A hashing algorithm used by a blockchain network creates hash codes at random [5].

On the blockchain network, mining computers compete to determine the hash value.

The hash rate on the blockchain network is a measurement of how many guesses are made per second.

When a miner predicts a number lower than or equal to the target hash's numerical value, the hash is considered “solved”.

The successful miner can add the following block to the Blockchain and get cryptocurrency rewards (often referred to as “block rewards”).

The hash rate of a blockchain network increases with the number of computers that connect to it and process hashes (guesses) on the network.

A PoW blockchain network with a high hash rate is more secure and healthy since there is less likelihood of an attack.

How to Measure Hash Rate?

The hash rate is known as the number of hashes [6] (or guesses) performed on a blockchain network per second. The hash rate increases with the size of the blockchain network.

Hash rate is often measured in terahashes, or 1 trillion hashes per second, because there are frequently hundreds (or thousands) of computers generating millions of guesses every second. For instance, the hash rate of the Bitcoin network is measured in terahashes per second.

Kilohashes per second (1,000/s), mega hashes per second (1,000,000/s), or gigahashes per second (1 billion/s) may be used to monitor smaller networks.

B.3. Why is Hash Rate Important?

Hash rate is crucial to gauge a blockchain [7] network's overall security and the difficulty at which miners must work to acquire block rewards. A malicious assault on the network is less likely to happen, with more blockchain miners vying to mine blocks.

The hash rate also influences the difficulty of mining a particular blockchain. As the hash rate rises, some blockchains make mining blocks more challenging. This implies that lone miners may be exceedingly difficult to compete in cryptocurrency networks with extremely high hash rates [7].

Moreover lastly, a cryptocurrency's popularity may be determined by its hash rates. A particular cryptocurrency network is more likely to experience growth and popularity as more computer power is committed to it.

C. What Is PoW Hash Rate?

As of October 2022, the hash rate on the Bitcoin network is around 240,000,000 terahashes per second (TH/s). In May 2011, the network achieved a hash rate of 1 TH/s for the first time, and since then, it has risen annually.

What Happens When the Hash Rate Changes (Increases or Decreases)?

On a PoW network, the hash rate serves as a barometer for miners' total network activity [8]. What it implies when the hash rate rises are as follows:

Block mining requires more computer horsepower

- , and the electricity used increases
- ; as the network grows too large for a single body to control, its security rises.
- As the hash rate rises, mining becomes significantly more challenging, and most blockchain network algorithms do the same.

A PoW blockchain network's hash rate dropping often indicates:

- There are fewer miners vying for block rewards and adding new blocks.
- When a group of miners with more than 50% of the network's hash rate modify the Blockchain, the network becomes less secure and more susceptible to a 51% assault.
- Computers used for mining use less energy.
- Block mining becomes less challenging as mining difficulty decreases.

Where can I view various cryptocurrency hash rates [9]?

Viewing the hash rates of well-known PoW crypto blockchain networks is possible in many locations. The hash rates of different cryptocurrencies are measured on websites like BitInfoCharts and others. Some of the most well-liked PoW hash rates are listed below:

- BITCOIN
- ETHEREUM
- ETHEREUM CLASSIC
- DOGECOIN
- LITECOIN
- MONERO

Through data-based learning and system interconnectivity, the integration of cutting-edge technologies like Cyber-Physical Systems (CPS), Big Data, Cloud Computing, Machine Learning, and Blockchain with healthcare services has enhanced performance and efficiency. However, because of the massive intake, sharing, and storage of healthcare data, it has also added complexity and brought its fair share of dangers. One of the significant difficulties facing the healthcare business is protecting sensitive data from cyberattacks while maintaining privacy through verified access. For this purpose, the use of Blockchain-based networks can lead to a considerable reduction in the vulnerabilities of the healthcare systems and secure their data. For this reason, the implementation of blockchain-based networks has the potential to significantly reduce the vulnerabilities of healthcare systems and safeguard their data.

Applications of blockchain technology in healthcare include secure medical data storage, log management, pharmaceutical supply chain management, and database administration and sharing [10], [11]. The authors [12] examine and identify the research possibilities for combining blockchain solutions with other cutting-edge technologies, including big data, algorithms, and IoT.

I also look at blockchain-based solutions to the security problems that healthcare institutions have. In [13], analyze the difficulties encountered when integrating blockchain technology into healthcare systems regarding security criteria such as stability, confidentiality, security systems, and compatibility. They recognise that these technological advantages for healthcare security come with difficulties, such as determining the data needs and personal privacy. In [14], we may examine the possibilities for blockchain technology in medicine and make the case that it can address issues with various forms of data, such EHRs. Dealing with blockchain technology's advantages not solely in aspects like reduced processing times, lower costs, and increased transparency but mostly in data security and privacy.

SECURITY

a. Blockchain security in the healthcare industry pros and cons [15].

For several reasons, distributed ledger technology is still in use today. The most important one is that it has facilitated both the emergence of cryptocurrencies over the past several years and the usage of un cryptographic currencies more straightforwardly. It is believed that the influence of the technology itself outweighs that of cryptocurrencies substantially. Thus, by scholars and professionals working in these disciplines, Blockchain's real potential is still being uncovered.

A new era of innovation is beginning for the healthcare sector with the introduction of Health 4.0. Integrating cutting-edge technologies like Big Data, Cloud Computing, Machine Learning, Cyber-Physical Systems (CPS), and Blockchain with healthcare services has improved performance and efficiency through data-based learning and system interconnectivity [16].

However, the widespread collection, exchange, and backup of healthcare data has also increased complexity and brought a fair share of risks. Safeguarding sensitive data from cyberattacks while retaining privacy through authenticated access is one of the healthcare industry's biggest challenges. Because of this, I am implementing blockchain-based networks that can significantly minimize healthcare systems' vulnerabilities and protect patient data. This essay answers the following queries to help readers better comprehend how blockchains may be used to protect healthcare data: what data are utilized, when do we need them, why do we want them, and who requires them? In order to provide a roadmap for future study topics that we may perform or, at the very least, instruct, we identify and investigate the technological limitations and legal difficulties associated with the adoption of blockchain-based medical data security.

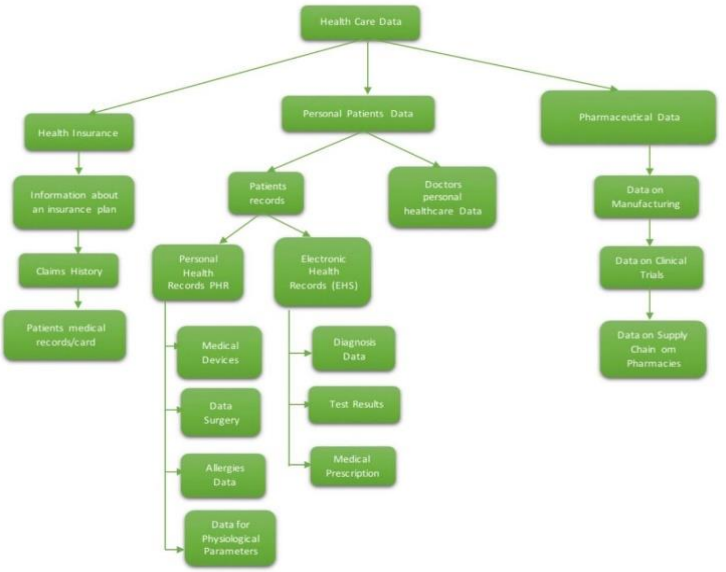

Fig. 2 Health care data (self edition)

b. Technical hurdles to blockchain adoption in the healthcare industry

One of the functional restrictions of blockchain technology is its inability to scale for huge networks. It isn't easy to store such a vast amount of data at each node. The authors of suggest storing just some data, such as metadata, hash values, and pointers on the Blockchain and other data on servers to address this problem. Scalability is only one problem; the privacy of healthcare data is another. Each node of a blockchain keeps a copy of the ledger since it runs on a distributed network. However, sharing copies of a patient's medical diagnosis reports throughout the network is not in the patient's best interest.

The concern about data privacy is thus another justification for a hybrid data storage solution based on Blockchain in the healthcare industry. Even if the entirety of the data is not shared throughout the network, everyone has access to the Blockchain's transaction data that is tied to each node's ID. Therefore, the Blockchain cannot safeguard the confidentiality of node activity. In addition to blockchain-based encryption, as we covered in the previous section, other encryption methods are used to protect user privacy. Modern blockchain-based systems have different access control mechanisms intended to handle data privacy issues. There is no mechanism to enforce these rules inside the network without using functionality outside the blockchain characteristics, even though they are integrated into the system through storage on the blocks. Various consensus algorithms used in Blockchain have specific limitations besides the overall functionality restrictions. The various consensus algorithms employed in blockchain technology have distinct limits in addition to the general functionality constraints. These limitations are universal and equally relevant to Blockchain in healthcare applications. Since the proof of work requires computing resources, most individual patients and small hospitals cannot afford them. Even for permission blockchains, the demand for computing resources goes against the idea of participant equality. Network congestion occurs for the PBFT consensus utilized in the Hyperledger blockchain because so many messages must be transmitted between the nodes. Patients now transmit personal healthcare data collected through smartphones and medical IoT devices.

Smart contracts allow for the execution of features like access control, privacy, recording, modification, and viewing healthcare data. Smart contracts greatly help task automation. However, a number of smart contract restrictions. Have a direct impact on how well healthcare data security operates. No one can alter a smart contract's code once it is stored on the Blockchain. As a result, before releasing, developers must look for vulnerabilities. Every validating node runs these contracts whenever they are requested to perform an action in order to validate the transactions. As every node has access to all the data the code utilises, it raises privacy concerns. Therefore, while creating a smart contract, additional care must be given to determining how much data and the encryption keys to supply.

c. Blockchain regulatory issues for healthcare data security

Among these, the privacy concern is one of importance. Due to the immutability feature of the Blockchain, past data cannot be deleted if a patient or an organization decides to quit the network. It violates the framework of the “right to be forgotten” provided under privacy rights in the majority of countries.

Systems for storing healthcare data on the Blockchain are not yet standardized . The many cutting-edge systems are used by the firms in accordance with their needs. Blockchain-using healthcare businesses have unique data storage formats, encryption methods, and consensus algorithms. Hospitals and other healthcare organizations find it challenging to interact as a result of interoperability problems across the blockchains. The requirement to move their data across chains creates a problem for the patients. Standard operating procedures for blockchain activities are therefore necessary.

CONCLUSIONS

In the healthcare sector, where sensitive patient data is involved, the necessity of cryptographic verification and majority approval before adding new blockchain blocks promotes openness and shared accountability. In terms of controlling who has access to and how their data is used, it offers the patients a number of advantages. By reducing the bottlenecks related to the system's centralized operation, it also simplifies the operations of doctors, healthcare organizations, and medical research facilities in terms of getting pertinent information. Blockchain eliminates the requirement for a reliable third party and places the burden of data security on all stakeholders through individual encryption. To fully secure, protect the privacy of, and ensure responsibility for the pertinent data, healthcare institutions now prioritize decentralizing systemic functioning [17]. In order to achieve the same goal, peer-to-peer networks built on blockchain technology are used extensively. None of the planned blockchain-based healthcare networks, however, are 100 per cent decentralized [10]. These systems' administrative nodes, which interfere with them, call for the study to achieve complete decentralization and full transparency. Healthcare blockchain-based systems require a sustainable incentive generation mechanism and sharing for the miners/validators in order to maintain the network. For the healthcare industry specifically, it is now difficult to keep all the data on the Blockchain. Additionally, data privacy is equally important. Therefore, just the metadata and hash values are saved on the Blockchain in place of all healthcare data.

In these circumstances, extra data encryption is implemented on top of the encryption offered by the Blockchain for data privacy. Blockchain-based networks can significantly contribute to data security for the future generation of healthcare systems, but this will require an ongoing study on scalability and encryption methods. In addition to technological difficulties, legislative issues, including the ownership of healthcare data and the need for a uniform inter-organizational operating format, exist. Specifically tailored to the data kinds, organizational hierarchies, and security concerns in the healthcare industry, the

REFERENCES

[1] J. Frankefield, “Merkle Root (Cryptocurrency) Definition,” Aug. 24, 2021. https://www.investopedia.com/terms/m/merkle-root-cryptocurrency.asp (accessed Nov. 10, 2022).

[2] L. Carlozo, "What is blockchain?," J. Account., Jul. 2017, Accessed: Nov. 10, 2022. [Online]. Available: https://www.journalofaccountancy.com/issues/2017/jul/what-is-blockchain.html.
[3] Z. Geylan, "Research: A deep-dive into Bitcoin hash rate, reasons behind increase, and whether it will rise again," Cryptoslate, Oct. 27, 2022. https://cryptoslate.com/research-a-deep-dive-into-bitcoin-hash-rate-reasons-behind-increase-and-whether-it-will-rise-again/ (accessed Nov. 10, 2022).
[4] G. Weston, "What is a Hash Rate? - 101 Blockchains," Aug. 12, 2022. https://101blockchains.com/hash-rate/ (accessed Nov. 10, 2022).
[5] H. Mirvaziri, K. Jumari, M. Ismail, and Z. M. Hanapi, "A new Hash Function Based on Combination of Existing Digest Algorithms," in 2007 5th Student Conference on Research and Development, 2007, pp. 1–6, doi: 10.1109/SCORED.2007.4451409.
[6] W. N. Suliyanti and R. F. Sari, "Evaluation of Hash Rate-based Double-Spending based on Proof-of-Work Blockchain," in 2019 International Conference on Information and Communication Technology Convergence (ICTC), 2019, pp. 169–174, doi: 10.1109/ICTC46691.2019.8939684.
[7] J. Hall, "Not a minor adjustment: Bitcoin mining difficulty soars 13.5% to new ATH," Oct. 10, 2022. https://cointelegraph.com/news/not-a-minor-adjustment-bitcoin-mining-difficulty-soars-13-5-to-new-ath (accessed Nov. 10, 2022).
[8] J. Wade, "Hash Rate," Jun. 10, 2022. https://www.investopedia.com/hash-rate-6746261 (accessed Nov. 10, 2022).
[9] Blockchain.com, "Charts - hash-rate," Nov. 10, 2022. https://www.blockchain.com/explorer/charts/hash-rate (accessed Nov. 10, 2022).
[10] M. Hölbl, M. Kompara, A. Kamišalić, and L. Nemec Zlatolas, "A Systematic Review of the Use of Blockchain in Healthcare," Symmetry (Basel)., vol. 10, no. 10, 2018, doi: 10.3390/sym10100470.
[11] V. de Aguiar et al., "Brain volumes as predictors of tDCS effects in primary progressive aphasia," Brain Lang., vol. 200, p. 104707, 2020, doi: https://doi.org/10.1016/j.bandl.2019.104707.
[12] S. Shi et al., "Association of Cardiac Injury With Mortality in Hospitalized Patients With COVID-19 in Wuhan, China," JAMA Cardiol., vol. 5, no. 7, pp. 802–810, Jul. 2020, doi: 10.1001/jamacardio.2020.0950.
[13] G. M. Gencer, C. Yolcu, F. Kahraman, and N. Saklakoğlu, "Effect of the surface nanocrystallization on tribological behavior of the Cu based bimetallic materials (CuPbSn)," Mater. Res. Express, vol. 6, no. 11, p. 116502, Sep. 2019, doi: 10.1088/2053-1591/AB43B3.
[14] R. A. Ali, E. S. Ali, R. A. Mokhtar, and R. A. Saeed, "Blockchain for IoT-Based Cyber-Physical Systems (CPS): Applications and Challenges," in Blockchain based Internet of Things, D. De, S. Bhattacharyya, and J. J. P. C. Rodrigues, Eds. Singapore: Springer Singapore, 2022, pp. 81–111.
[15] Codescrum, "Key Pros and Cons of Blockchain in Healthcare," Jul. 01, 2021. https://www.codescrum.com/blog/key-pros-and-cons-of-blockchain-in-healthcare (accessed Nov. 10, 2022).

[16] N. Alkhaldi, "Top Blockchain Use Cases in Healthcare, Advantages, and Challenges — ITRex," Mar. 23, 2022. https://itrexgroup.com/blog/blockchain-use-cases-in-healthcare-advantages-challenges/ (accessed Nov. 10, 2022).
[17] EDPB, "EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space," 2022.