Blockchain Enabled Secure Transaction using Hash Functions in Healthcare Data

[1]Alan Sunil, [2]Smitha Anu Thomas

[1]Scholar, [2]Professor
dept. of computer sciences, Nirmala College, Muvattupuzha, India

Abstract: **Blockchain can be defined as an interconnected chain of data blocks that allows the creation of transaction records based on a managed distributed consensus protocol without a central authority. Hash functions are the most important element in the security foundations of blockchain technology. This paper presents an insight into the application of cryptographic hash functions in securing and managing healthcare data stored using blockchain technology. Over the last few decades, the healthcare industry has continuously grown, with hundreds of thousands of patients obtaining treatment remotely using smart devices. Data security becomes a prime concern with such a massive increase in the number of patients. Numerous attacks on healthcare data have recently been identified that can put the patient's identity at stake. For example, the private data of millions of patients have been published online, posing a severe risk to patients' data privacy. However, with the advent of Industry 4.0, medical practitioners can digitally assess the patient's condition and administer prompt prescriptions. However, wearable devices are also vulnerable to numerous security threats, such as session hijacking, data manipulation, and spoofing attacks. Attackers can tamper with the patient's wearable device and relays the tampered data to the concerned doctor. This can put the patient's life at high risk. Since blockchain is a transparent and immutable decentralized system, it can be utilized for securely storing patient's wearable data.**

Keywords: Blockchain, Hash function, Health technologies, Artificial intelligence.

I. INTRODUCTION

A blockchain is a distributed ledger with growing lists of records (blocks) that are securely linked together via cryptographic hashes. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree, where data nodes are represented by leaves). Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. An *asset* can be tangible (a house, car, cash, land) or intangible (intellectual property, patents, copyrights, branding). Virtually anything of value can be tracked and traded on a blockchain network, reducing risk and cutting costs for all involved. The data is chronologically consistent because you cannot delete or modify the chain without consensus from the network. As a result, you can use blockchain technology to create an unalterable or immutable ledger for tracking orders, payments, accounts, and other transactions. The system has built-in mechanisms that prevent unauthorized transaction entries and create consistency in the shared view of these transactions. Many researchers have made pivotal contributions on the significance of blockchain but the research of blockchain is still in its infancy. The study reviews the current academic research on blockchain, by conducting a clustering analysis to identify the research areas of economic benefit, blockchain technology, initial coin offerings, fintech revolution, and sharing economy. In 2008, Satoshi Nakamoto proposed the concepts of bitcoin and blockchain, describes how cryptology and an open distributed ledger can be combined into a digital currency application. The widespread adoption of the digital currency bitcoin in financial transactions has led to many business innovations and value.

The advent of blockchain technology attracted the attention of the entire scientific community. It is a shared public ledger that securely stores wearable healthcare data in an immutable manner to improve data privacy and establish trust between various entities of the healthcare systems. Ref. introduced a medical care information preservation system that considered the complete data storage process in wearables and medical center servers. The procedure is secure and follows the Health Insurance Portability and Accountability (HIPAA) privacy and security requirements. Their suggested approach employed the advanced chaotic map technique key negotiation, reducing the amount of processing required, and achieving lightweight quantification. It also takes advantage of blockchain technology's characteristics that secure healthcare data from data manipulation attacks and boost data security. Then, the authors offered a blockchain and smart contract-based trustworthy and transparent medicine supply chain to prevent doctors' prescription information from being manipulated by attackers.

II. FEATURES

Blockchain features can be summarised as follows: **Decentralisation**: The same information of the blockchain is replicated and distributed by the nodes in the network, which can also independently validate this information without a centralised authority.

Immutability (tamper-proof): A permanent record of transactions (ledger) is maintained by the peers. Once a block is upended, it cannot be modified as it is cryptographically sealed in the ledger. This creates trust in the transaction record.

Transparency: The ledger contains a full transaction history. As the blockchain is an open file, anyone can access it and audit transactions. This ensures provenance under which asset lifetimes can be tracked.

Chronological (time stamped): The cryptographic approach in blockchain links blocks together in a chronological chain providing a trial of the underlying transactions.

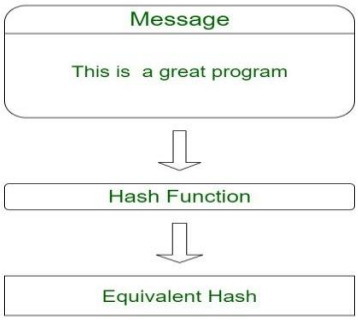
III. BLOCKCHAIN TECHNOLOGY AND HASH FUNCTIONS

A comprehensive way to secure the message block and to connect the blocks in a chain is to use hash functions. Hashing is the process of converting a data or message into a digest or hash using cryptographic hash functions for the irreversible conversion

of the message. In blockchain, each block contains its own block hash and a hash of its previous block, thus creating cryptographically secured linear chain of blocks. The hash function takes the input of variable lengths and returns outputs of fixed lengths.

In simple terms, hashing means taking an input string of any length and giving out an output of a fixed length.

A hash function is a mathematical function that takes an input string of any length and converts it to a fixedlength output string. The fixed-length output is known as the hash value.



In the context of cryptocurrencies like bitcoin, the transactions are taken as input and run through a hashing algorithm (bitcoin uses SHA-256) which gives an output of a fixed length.

Let M be given as an arbitrary size input message. The hash function H is applied to the message M to encrypt and generate a message digest as output which is a fixed-size hexadecimal output.

H(M) = Digest

Cryptographic hash functions are one-way functions which are irreversible and the message cannot be generated back using the digest. There are a bunch of cryptographic hash functions such as SHA-224, SHA-256, SHA-512, KECCAK256, Whirlpool, etc. The family of SHA comprises four SHA algorithms: SHA-0, SHA-1, SHA-2, and SHA-3.

- SHA-0 is a 160-bit hash function that was published by the National Institute of Standards and Technology in 1993.
- SHA-1 was designed in 1995 to correct the weaknesses of SHA-0. In 2005, a method was found to uncover collisions in the SHA-1 algorithm due to which long-term employability became doubtful.
- SHA-2 has the following SHA variants, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256. It is a stronger hash function and it still follows the design of SHA-1.
- In 2012, the Keccak algorithm was chosen as the new SHA-3 standard.
- SHA-256 is the most famous of all cryptographic hash functions because it's used extensively in blockchain technology.

IV. BLOCKCHAIN AND HEALHCARE DATA MANAGEMENT

Blockchain technology has tremendous potential in managing the data of patients. The advent of internet and allied technologies has led to the monitoring and treatment of patients remotely using smart devices. Medical practitioners can digitally assess and administer the patient recommending prompt prescriptions. But the smart devices are vulnerable to security threats, data manipulation and attacks. Since blockchain is a transparent and immutable decentralized system, it can be utilized for securely storing patient's data thus increasing the accuracy of Electronic Health Records (EHR).

Blockchain technology is a robust framework for securely storing the medical data of patients is very important in healthcare. The sensitive data can be controlled and managed in encrypted form using hash functions. Therefore, sharing and accessing the control of healthcare data of patients is possible.

Issues Targeted	Solution Proposed	Pros	Cons
Automated health record system using blockchain	The proposed system exchanges health information on the blockchain to create a smart e-health system	The system utilizes a modified Merkle tree data structure which provides secure and fast access of patient logs	The system does not consider the possible manipulation of patient data by attackers.
Bribery self-mining in blockchain	Proposed a new selfish mining scheme and ways to tackle it	The system proposes a unique way of selfish mining in Ethereum which is more efficient than others	The proposed scheme has lower ethereum costs and higher rewards, leading to more harmful attacks on healthcare systems.
Blockchain for healthcare	Blockchain-based 5G healthcare architecture	The solution utilizes the 5G technology alongside blockchain, which provides ultra-low latency and high data rate, which are crucial for healthcare systems.	The proposed framework does not check whether the data received by the blockchain is tampered with or not.

Fig 1: Blockchain Solutions for Health-care Data Management

V. PROPOSED METHODOLOGY

The authors proposed an automated health record system that utilizes blockchain technology. The proposed framework is designed to exchange health information on the blockchain in order to create a smart e-health system. The system uses a modified Merkle tree data structure for faster and more secure access to patient logs. The disadvantage, however, is that the proposed system did not consider the possibility of malicious data being uploaded into the blockchain. Attackers can manipulate the patient's data and upload it onto the blockchain, which can cause many problems in the system. The authors of has proposed a bribery self-mining

system in the blockchain that works on Ethereum. The proposed system describes a new way of essentially gaining higher rewards and spending less Ethereum. The system is tested on a simulated healthcare system, and it is seen that harmful attacks can be made on a healthcare system due to higher rewards and lower spending costs. The proposed system has been developed to detect intrusion in healthcare systems using deep learning and blockchain. The demerit of this system is that it does not consider the patient's health data, which can threaten the patient's life if incorrect data are fed into the blockchain. Therefore, there is a requirement for a blockchain and AIbased secure and trusted framework that analyses different security attacks from wearable devices and improves the security and privacy of the healthcare industry. The blockchain layer is in charge of securing data stored in the blockchain to tackle data injection attacks [36– 38]. To check the validity of the data, a smart contract is employed. Smart contracts are programs executed based on the satisfaction of certain conditions and are stored in the blockchain network. The data are initially routed through a smart contract, determining who has access to the information. Blockchain is particularly important in the healthcare industry because the system protects sensitive data, which is very valuable in the field of healthcare. With the growth of electronic medical records, the healthcare industry is continuously attempting to secure patient, hospital, insurance, and billing records. In addition, with so much data available, keeping track of it all while maintaining privacy is difficult. Blockchain's essential properties, such as transparency, immutability, distributed network, and reliability, strengthen security and offers trust in healthcare systems. In healthcare systems, it is used to monitor the manufacturing of prescription medications and their safety. It provides a platform for storing patient medical records that practitioners can quickly access to give remote medical aid. It is utilized to lessen the risk of fraud and inaccuracy in the medical industry by expediting qualification verification. In the HEART, the patient's health records are only sent by the smart contract to be stored on the blockchain. The patient and the doctor can only access the data. If required, the doctor can prescribe medication and also suggest necessary treatment to the patient. Figure 5 shows the implementation of the aforementioned smart contract for the HEART. The smart contract has four major functionalities: User, health Data, prescription and view Patient Data. The User function is responsible for checking the type of user, i.e., whether they are a patient or a doctor. If the user is a patient, the wearable device automatically enters the patient's health data in the health Data function. This data is then stored onto the blockchain and can be viewed either by the patient or the doctor using the view Patient Data function. The user must enter a unique patient ID to view the patient's data. If the user is a doctor, they can use the prescription function to enter the medication, if necessary, to be given to the patient and also provide insights into what kind of treatment is necessary for the said patient. These functionalities are shown in Figure 5c and Figure 5d, respectively. If any unauthorized user tries to view a patient's data, a warning message is shown, and the patient's data will not be visible. Furthermore, the healthcare data are stored inside the interplanetary file system (IPFS)based public blockchain. A Merkle Tree or Merkle Directed Acyclic Graph, similar to the one used in the Git Version Control system, is employed inside IPFS to efficiently track changes to files on a network in a decentralized manner. Each data element is identified by the cryptographic hash of its contents, known as content-addressing to improve the response time and scalability of the blockchain network. Each block contains a header, which includes metadata such as the timestamp, the hash of the previous block, and the nonce (a value used in the mining process). The block also contains a list of validated transactions, and a Merkle Tree root, which is a single hash that represents the entire collection of transactions in the block.

Furthermore, each block also has a unique digital signature, called a "block hash", which Mathematics 2023, 11, 637 14 of 20 is generated using a cryptographic hashing algorithm. The block hash is based on the contents of the block, including the transaction data and the previous block's hash. To facilitate secure, transparent and accountable sharing of patient data, three distinct components are proposed.

1. Identification and Authentication Management of the patient. A user wishing to access personal data first needs to establish some kind of identifier or token. The token encapsulates a particular attribute to be registered with the Identity Manager, which is a blockchain contract used to store the tokens on blockchain. When the data provider seeks to authenticate a user, the user must be able to verify that the token in question is valid.
2. Authorisation or access management. The user can use the authenticated token to assert to the data provider that they are entitled to access a particular piece of data. Upon authorisation, Access Control Manager (ACM), which is a blockchain contract used to store and evaluate access control policy on blockchain, processes the user's request and provides them with a secret and the encrypted data.
3. Logging and Monitoring. Only authorised users can use the secret to reconstruct the key and decrypt the data based on a cryptographic approach. As part of the decryption process, the system generates a data access log. The system maintains all logs along with other information in the Log Storage for accountability purposes.

The blockchain type used in a healthcare system is a private or a consortium (public permissioned) blockchain. This is expected for healthcare as it is desirable to have control over access and writing to the blockchain and it is not desirable that writing (adding blocks to the blockchain) could be done by anyone.

Despite of all these features, implementation of blockchain has numerous disadvantages. Lack of standardization is an important challenge that hinders the wide acceptance of blockchain as solution in healthcare domain. Even though decentralized architecture is suitable for ensuring the interoperability in health care applications, there is a potential threat about the privacy as the data is stored and retrieved from a public ledger. The amalgamation of Artificial Intelligence and IoT Based blockchain solutions are popular in healthcare sector due to the wide use of mobile devices in remote health monitoring. But these solutions provide limited scalability, computationally expensive and provide additional overhead due to inadequate computational capacity of IoT devices like sensors. The management of keys, used by cryptographic techniques for ensuring the data privacy in blockchain applications is another issue that is yet to be resolved.

VI. CONCLUSION

The adoption of blockchain technology in healthcare domain has redesigned the aspect of healthcare applications. Usage of blockchain helps to time stamp the records so that no one can tamper with it. It gives the patient the right to decide regarding who

should have access to data and the how much information should be shared. It can be concluded that the cryptographic features hashing, public-private key pairs, and the digital signatures together constitute the foundation for the blockchain by securely linking blocks and ensuring reliability and immutability of the data stored on the blockchain. For the security of blockchain systems, we can increase the complexity of hash operations and increase the length of hash output.

VII. REFERENCES

1. X. Zhan, H. Yuan and X. Wang, "Research on Block Chain Network Intrusion Detection System," 2019 International Conference on Computer Network, Electronic and Automation (ICCNEA), Xi'an, China, 2019, pp. 191-196. doi: 10.1109/ICCNEA. 2019.00045.
2. D. Tse, K. Huang, B. Cai and K. Liang, "Robust Password-keeping System Using Block- chain Technology," 2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), Bangkok, Thailand, 2018, pp. 1221-1225.doi: 10.1109/IEEM.2018.8607284
3. C. H. Lee and K. Kim, "Implementation of IoT system using block chain with authentication and data protection," 2018 International Conference on Information Networking (ICOIN), Chiang Mai, Thailand, 2018, pp. 936-940.doi: 10.1109/ICOIN. 2018.8343261.
4. S. Niu, L. Chen and W. Liu, "Attribute-Based Keyword Search Encryption Scheme with Verifiable Ciphertext via Blockchains," 2020 IEEE 9th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), Chongqing, China, 2020, pp. 849- 853. doi: 10.1109/ ITAIC49862. 2020.9338962.
5. Zhang, Aiqing, and Xiaodong Lin"Towards secure and privacy- preserving data sharing in e-health systems via consortium blockchain." Jour-nal of medical systems 42, no. 8 (2018)
6. Chelladurai, U.; Pandian, S. A novel blockchain based electronic health record automation system for healthcare. J. Ambient. Intell. Humaniz. Comput. 2022, 13, 693–703. [CrossRef]
7. Mistry, C.; Thakker, U.; Gupta, R.; Obaidat, M.S.; Tanwar, S.; Kumar, N.; Rodrigues, J.J.P.C. MedBlock: An AI-enabled and Blockchaindriven Medical Healthcare System for COVID-19. In Proceedings of the ICC 2021—IEEE International Conference on Communications, Montreal, QC, Canada, 14–23 June 2021; pp. 1–6. [CrossRef}
8. Wang, Y.; Wang, Z.; Zhao, M.; Han, X.; Zhou, H.; Wang, X.; Koe, A.S.V. BSM-ether: Bribery selfish mining in blockchain-based healthcare systems. Inf. Sci. 2022, 601, 1–17. [CrossRef]