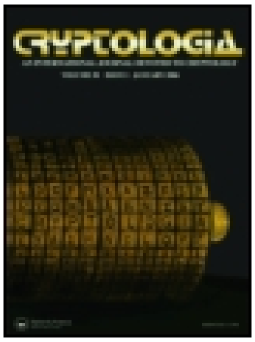

Cryptologia

ISSN: 0161-1194 (Print) 1558-1586 (Online) Journal homepage: https://www.tandfonline.com/loi/ucry20

Securing and authenticating healthcare records through blockchain technology

Prateek Pandey & Ratnesh Litoriya

To cite this article: Prateek Pandey & Ratnesh Litoriya (2020): Securing and authenticating healthcare records through blockchain technology, Cryptologia, DOI: 10.1080/01611194.2019.1706060

To link to this article: https://doi.org/10.1080/01611194.2019.1706060

Published online: 30 Jan 2020.

CRYPTOLOGIA
https://doi.org/10.1080/01611194.2019.1706060

Taylor & Francis
Taylor & Francis Group

Securing and authenticating healthcare records through blockchain technology

Prateek Pandey and Ratnesh Litoriya

ABSTRACT
Healthcare data is important in making critical policy decisions, patients care, and medical diagnostics to name a few. Due to the importance and market demand, healthcare data is also vulnerable to cyber attacks. The centralized record keeping systems expose a single node for the attackers to attack. A decentralized system is computationally expensive but has the ability to be revolutionary by keeping the patient at the core and providing security, transparency, privacy, and interoperability of the electronic healthcare data. A blockchain is such an implementation of a distributed and decentralized system using reliable cryptographic algorithms. This paper proposes a secure blockchain based architecture tailored specifically to cater to the needs of e-healthcare systems.

KEYWORDS
blockchain; distributed computing; EHR; healthcare

1. Introduction

Healthcare data is required to be managed electronically for efficient storage, sharing, protection, and analysis. Healthcare data, if available, provides for a holistic view of the patient's healthcare, personalized treatment, policy-making based on the population health, and analyze physician activities to streamline with the organization goals (Ward, Marsolo, and Froehle 2014; Ristevski and Chen 2018). Predictive analytics on the healthcare data provides insights to the marketing personnel to design an effective marketing campaign that saves time, efforts, and money of the organization.

The healthcare information is much in-demand by the fraudsters because it is hard to detect identity theft in healthcare. This is unlike a credit card, which can be blocked on request if stolen (Snell 2018). The healthcare data is confidential by nature and any leaks or compromises may severely affect the patient's privacy. Thus, a system is required that ensures patient's privacy and is secure, transparent, and undisputedly acceptable to all at the same time.

The conventional data-sharing systems are centralized and possess an inherent problem of a single point of failure. A decentralized system has

CONTACT Ratnesh Litoriya ✉ litoriya.ratnesh@gmail.com Department of Computer Science & Engineering, JAYPEE University of Engineering & Technology, Raghogarh, Guna, India.
Color versions of one or more of the figures in the article can be found online at www.tandfonline.com/ucry.

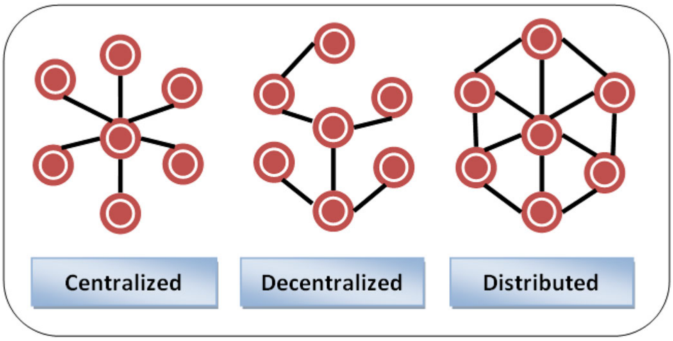

Figure 1. Types of electronic record-handling system.

multiple coordinators so that, if some coordinator nodes in the network collapse, then the individual nodes still maintain communication via other coordinators (Figure 1). Such networks withstand multiple points of failure until the network is partitioned (Rehman 2017). Further, distributed systems offer collective computation or information sharing by the network nodes.

A decentralized computation and information-sharing platform that enables multiple authoritative domains who do not trust each other to cooperate, coordinate, and collaborate in a rational decision-making process is regarded as a blockchain network (Atzori 2015).

Figure 2 represents an ecosystem consisting of health organizations as consumers and producers and patients as the direct consumers of electronic health records (EHR). Each and every transaction (access or storage) is accurately time stamped and becomes a part of a long chain or everlasting temper-proof record. Transactions of EHR on a blockchain network can be made transparent and privacy preserving at the same time. Security of transactions is an intrinsic property of the blockchain network. We propose a secure architecture in this article that exploits the intrinsic benefits of using blockchain and streamlines the management of EHR to suit the blockchain network.

Section 2 discusses the recent review of the available literature on blockchain and EHRs. Section 3 explains the underpinnings of the proposed architecture, followed by Section 4 describing the conceptualization and design of the proposed system. Implementation is detailed in Section 5 and the results are also discussed. The conclusion and the scope of future work are presented in Section 6.

2. Literature review

The sustainability and effectiveness of healthcare systems in the future will undoubtedly require better operational efficiencies. Essential to achieving

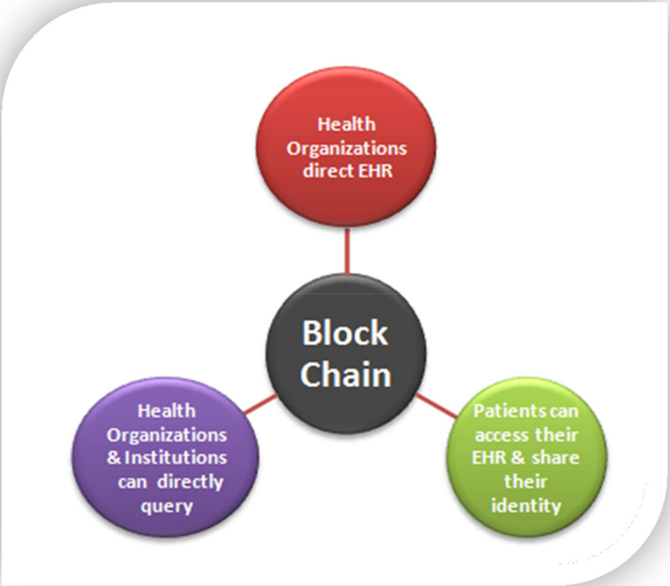
Health Organizations direct EHR
Block Chain
Health Organizations & Institutions can directly query
Patients can access their EHR & share their identity

Figure 2. Ecosystem of blockchain in healthcare.

this is the ability to integrate the massive amount of available health-related data from conventional sources, EHR, and other health data from different applications.

At the abstract level, blockchain technology can be defined as a platform for digital exchange, where the digital exchange is carried out without involving a traditional intermediary. The distributed ledger-based blockchain technology has drawn the attention of various stakeholders for its capabilities of handling data by respecting security and decentralization—the relatively successful implementation of blockchain in the financial domain has forced various businesses to explore the potential of this robust technique in their respective domains.

The health-related information of individuals can exist in several systems and sharing such information requires many points to collaborate amid entities. Hence, the healthcare domain is unanimously recognized as one such industry aiming to unlock the advantages of the blockchain. In the healthcare domain, blockchain has been admired for assuring susceptible data security and ensuring valid and certified access to EHR. Furthermore, with this emerging technology, it is perhaps almost unfeasible to falsify records or corrupt the data. However, some experts think that blockchain is one of the most misapprehended technologies and that all sorts of applications are not necessarily realistic (Rucker 2018).

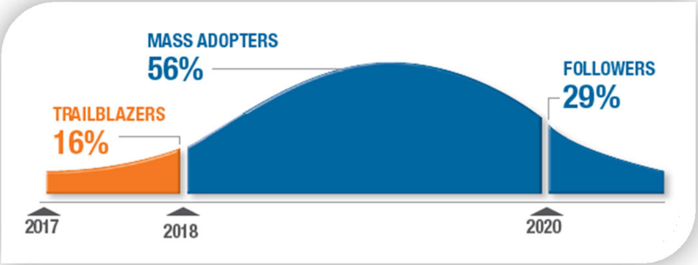

Figure 3. Blockchain adoption scenario in healthcare (IBM Institute for Business Value, 2016).

Blockchain has acquired interest as a platform to get improved transparency and authenticity of healthcare information all the way through various use cases, from streamlining claims processing to upholding permissions in EHR. Numerous opportunities are present in the area of healthcare where blockchain can help improve privacy, security, and interoperability of health data of the patient.

The rate of blockchain adoption is increasing; organizations are moving very fast to deploy this inimitable technology in maintaining EHRs and, indeed, even appear to have a lead on the financial industry. According to a survey conducted by IBM in 2016, 16% of healthcare institutions are trailblazers, prepared to popularize blockchains at scale in 2017. The majority of healthcare organizations would become mass adopters by the year 2020 (IBM Institute for Business Value 2016). Figure 3 illustrates the expectations of healthcare respondents regarding their adoption of blockchains in production and at scale.

Various studies on the blockchain application in the diverse field have been carried out (Christidis and Devetsikiotis 2016). A comprehensive review of the blockchain architecture and the different mechanisms concerned in this technology is also presented (Zheng et al. 2017; Yin et al. 2017). A few research articles also provide an overview of blockchain highlighting its big data and industrial application (Ahram et al. 2017; Karafiloski and Mishev 2017). A systematic review containing a detailed analysis of blockchain application and related research topics are discussed (Yli-Huumo et al. 2016; Conoscenti, Vetro, and Martin 2016).

The applicability of blockchain technology in the healthcare sector has been described extensively in many articles and reports (Krawiec and White 2016; Schumacher 2017; Nugent, Upton, and Cimpoesu 2016). The fundamentals of blockchain and demonstration of existing and future applications of this novice technology within the healthcare industry are described in detail (Angraal, Krumholz, and Schulz 2017; Alhadhrami et al.

2017). Matthias Mettler (2016) focused on various opening points for Blockchain technology in the healthcare industry. The author illustrated potential goals and influences related to this boisterous technology by taking the various example of public healthcare management, drug imitation in the pharmaceutical sector, and user-oriented medical research.

Zang et al. (2018) explain the applicability of blockchain technology in healthcare by discovering the prospective use cases of blockchain in healthcare. Further, a case study DApp for Smart Health (DASH) is developed to investigate the effectiveness of applying this secure technology to the healthcare field. The authors also evaluated design considerations when blockchain is applied in healthcare. A distributed model OmniPHR (Roehrs et al. 2017) is developed to integrate patient health records for patients' and healthcare providers' use. An architectural model to support a distributed PHR is proposed, which enables patients to maintain their health history from an integrated point of view, from any location.

Kuo et al. (Kuo, Kim, and Ohno-Machado 2017) identified various benefits of blockchain technology in comparison with conventionally distributed databases for biomedical and healthcare applications and presented a general idea of the most modern applications of blockchain technology in the healthcare/biomedical domain (for instance, healthcare data ledger, better insurance claim processes, etc.).

Stan (Sater 2019) talks about architectural considerations for a healthcare data exchange based on the blockchain. The present regulatory environment is also taken into consideration. Engelhardt et al. (2017) describe some tangible examples of the blockchain application in the health sector. Future challenges and other issues are also discussed.

To assure the anonymity and immutability of the information and to meet the requirement of the structure of blockchain, multiple authorities are introduced into Attribute-based signature (ABS) and put forward an MA-ABS scheme (Guo et al. 2018). The objective is to preserve the privacy of the patient in an EHR system.

Liu et al. (2017) describe blockchain architecture as a novel system solution to provide an unswerving mechanism for safe and proficient exchanges of medical records. To meet the rising demand for healthcare record management systems an advanced blockchain approach is introduced. A framework for cross-domain image sharing (Patel 2018) utilizing blockchain is developed as a distributed data store to set up a ledger of patient-defined access permissions and radiological studies. A blockchain-based framework Ancile (Dagher et al. 2018) is proposed, and is intended for interoperable, secure, and efficient access to EHR by patients, providers, and other stakeholders, while at the same time upholding the privacy of patients' information. This framework exploits smart contracts in an Ethereum-based blockchain for quick access control and data obfuscation. For enhanced security, Ancile uses advanced cryptographic techniques.

It can be stated apparently from the literature review that blockchain is considered to have extraordinary potential in the field of healthcare. The efforts should be applied to the EHR management that could benefit from the possibility to connect incongruent systems and enhance the precision and security of EHR. This innovative decentralized blockchain technology can be utilized to support access control, medicine prescription, pregnancy, or any severe-disease data management, clinical trials, anti-counterfeiting drugs, and control of an audit trail of health-related activities.

The majority of the articles presented theoretical research, for example: architecture, a framework, or a model for use in EHR management and employing a blockchain. Moreover, technical details concerning the used blockchain essentials are not specified like blockchain type, platform, consensus algorithm, or the making of smart contracts. The literature indicates that blockchain technology is still in relative immaturity, predominantly in healthcare. Simultaneously, research on blockchain technology and its employment in healthcare-data management is increasing. New and more efficient ways for employing this neophyte technology in electronic health record management can still be found and researched.

3. Proposed architecture

Multiple devices in a network are not equally efficient—some are slower or even unresponsive sometimes. Multiple network systems have their own limitations, like heterogeneous latencies, and designing a distributed or decentralized system is challenging under such constraints.

We propose a decentralized secure architecture for managing electronic records by keeping in view the exclusive needs of the healthcare sector. The idea is inherited from the existing blockchain architectures; therefore, it has a few similarities as well as differences from it. The proposed architecture is based on the Hyperledger fabric by IBM.

Ethereum and Hyperledger are the two popular blockchain platforms being used in the domain of healthcare (Macdonald, Liu-Thorrold, and Julien 2017; Kuo, Zavaleta Rojas, and Ohno-Machado 2019). Ethereum works on ‘Proof of Work (PoW)’—a consensus algorithm that consumes power and resources, while Hyperledger doesn’t. Another reason for using Hyperledger as the underlying platform is confidentiality. Hyperledger keeps a contract confidential between two parties—an important requirement for exchanging health data; Ethereum, on the other hand, makes contracts public.

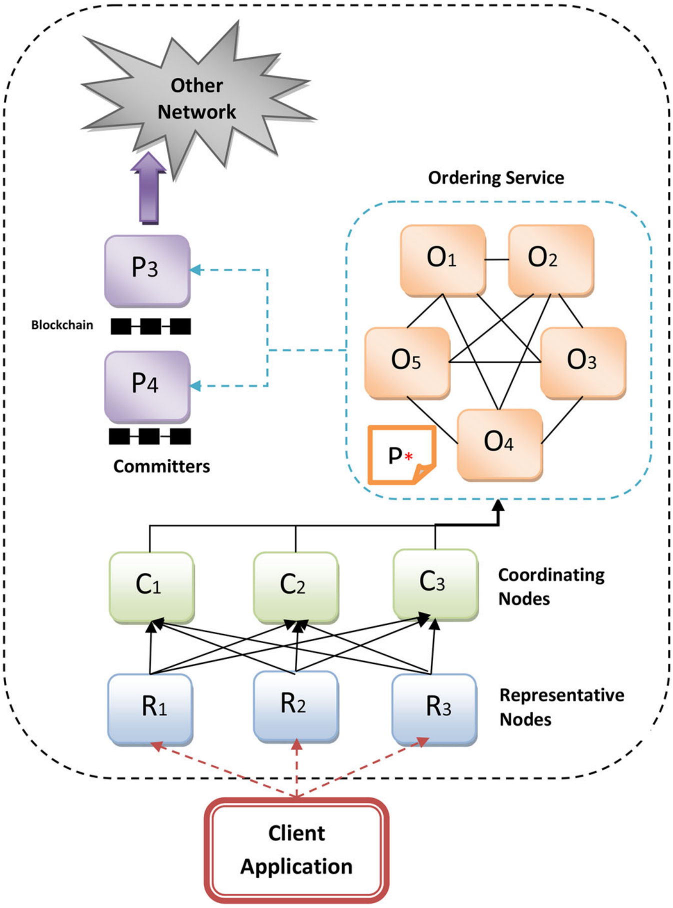

Figure 4. Architecture of blockchain perspective in health care domain.

The architecture is presented through Figure 4. The architecture is decentralized in the sense that there are various participating nodes in the network performing the duties that would otherwise be performed by a single node in a centralized system. Thus, the proposed system is intrinsically fail safe. Participating nodes in the proposed system maintain a ledger of the past transactions. This means the nodes need to have sufficient disk space and computing power to fulfill the network needs. Five kinds of nodes are present in the network: clients, representatives, coordinators, organizers, and the committers. Clients request network for required services.

Representatives handle clients' requests and validate them before endorsement. Coordinators verify the endorsements and reject or accept proposals for further ordering. Organizers receive verified proposals from multiple coordinators and organize the transactions into blocks and broadcast those newly created blocks to the peer coordinators and committers, which further propagate them into the network. In this way, the most updated state is replicated to the entire network. A block is a structure that

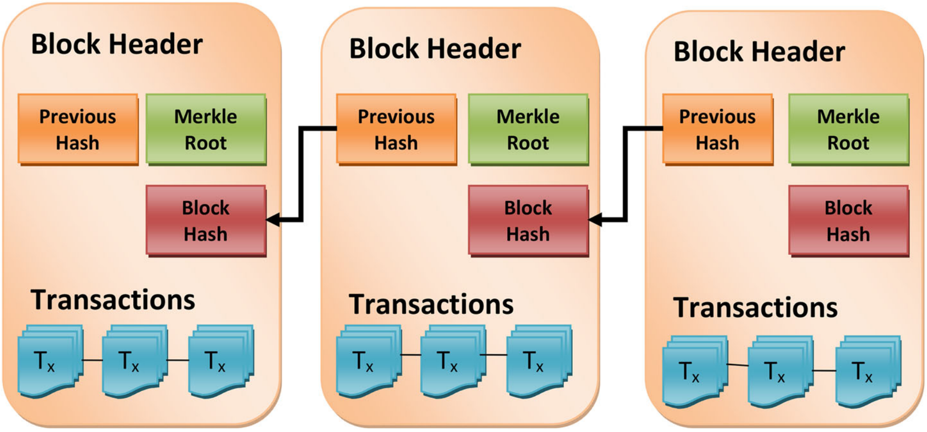

Figure 5. A typical structure of a block and blockchain.

contains transactions and a header (Figure 5). The block header consists of a time stamp (when the block was created), the current block's hash, the previous block's hash, and the Merkle root. The hash for the current block is computed by using the hash of the previous block and Merkle root of the transactions (Macdonald, Liu-Thorrold, and Julien 2017).

Thus, a new block is always appended to the previous block forming a link or chain of blocks arranged chronologically (Figure 5). The architecture requires that every participating node in the network maintains a local but up-to-date copy of this chain of blocks. This arrangement makes the transactions tamper proof. If an attacker manipulates a transaction to his favor, the Merkle root representing the hash of all candidate transactions gets changed, and hence the hash for that particular block. Because the attacked block is also linked to the next block using a hash, and so on, a state of disharmony will arise and the network will not accept this change. In this way, the whole of the network participates in providing security and ensuring the integrity of the transactions involved. The next section presents a design to realize this architecture.

Every entity involved in the network is identified by an authentication and authority agency (AAA). AAA ensures that only the verified entities perform their duties as per the authorized access.

4. Conceptualization and design

We assume, for this case, that a healthcare provider has a number of hospitals, doctors, and other staff. Hospitals, doctors, staff, and patients are identified by special identification keys. Prescriptions, reports, invoices, insurance claims, birth and death certificates, etc. are the typical electronic documents generated and exchanged on a routine basis and are described as transactions. We define a size of 20 KB for a block, which can roughly contain around 10 transactions. A time limit of 5 minutes is also placed, which means even if a developing block contains only one transaction, it will be committed in the ledger after 5 minutes. In this way, transactions would not have to wait for an undetermined time to commit.

The network is closed in the sense that only those who are authorized can propose or look into the transactions. The privacy of the patient's data can be maintained by removing identifying information, particularly the name and contact details or by using an independent review process to make sure the reason for using patient data is appropriate (Kuo, Zavaleta Rojas, and Ohno-Machado 2019). The privacy is implemented into the system by using a hash of the patient ID provided by the AAA. Every document over the network is stored and identified by using this hash only. So, due to the one-way property of hashing, the patient's information can't be traced by looking at the electronic document.

Once a document is created or exchanged, this information has to be logged into the distributed network. A client informs such transactions to the representatives and each representative verifies the source and privileges of the transaction. This scenario is explained using step 1 to step 4.

Step 1: Suppose an X-ray operator performs an X-ray over a patient with patient ID 001. The client (X-ray operator) would sign this transaction using his private key before proposing it to the representative nodes. The representative nodes check the authenticity and authorizations of the client and then endorse the proposal with an 'E' flag or refuse it with an 'R' flag. Representatives send the proposals to the coordinators with their endorsements or refusals.

Step 2: The coordinators ensure that the client's proposal receives sufficient approvals as per the endorsement policy. If a client proposal does not comply with the policy, coordinators do not forward the transaction toward organizers. The coordinators also perform an additional task of verifying the transactions using smart contracts. For example, a smart contract would check whether this transaction "*X-ray film produced for pid 1bcb9cefbc5ef8afn5ad4d4ff74b3dae @ ….\hospital\reportstore\x-ray\1bcb9cefbc5ef8afn5ad4d4ff74b3dae-21-01-2019-1400.xry*" is verified by performing a lookup into the X-ray store: lookup ("….\hospital\reportstore\x-ray\1bcb9cefbc5ef8afn5ad4d4ff74b3dae -21-01-2019-1400.xry"). If this lookup results into an affirmation, the transaction is said to be verified. Smart contracts may also be signed between the patients and the healthcare provider over the mutually agreed terms and use.

Step 3: The organizers then receive the transactions from the coordinators, order the transactions according to their timestamps, and create a new block of transactions by consensus. Organizers do not possess the copy of the distributed ledger; instead, they keep a consistent copy of the last block hash.

Step 4: Organizers then multicast the newly formed block to each of the coordinating and committing nodes, which once again validate the transactions inside the block and then commit and update their ledgers accordingly. This second validation is to make sure that a transaction is not invalidated in between.

The proposed architectural design has some distinguishing features that make it scalable, resilient, business oriented, transparent, and private:

1. In the proposed design, the onus of maintaining the public ledger lies only on the committing nodes, though coordinators may also keep ledger copies. Organizers maintain a copy of the last block hash only—not the complete ledger. This enables using a generalized organizing service for serving multiple organizations or using third-party organizing services without jeopardizing the security of the past data.
2. The representative nodes do the work of a doorkeeper to check whether a transaction is authorized and coming from an authentic source. This helps to apply business logic at the early stage by restricting wrong transactions from entering further into the system.
3. Use of hash values for storing and exchanging health information provides privacy yet offers transparency to the system. Transactions are visible to all the participants holding the ledger, but none can figure out the identity of a patient by looking at the transaction.
4. A committer in the proposed design may also be a part of another organizational hierarchy and can multicast the new blocks to other peers. Thus, the system is intrinsically scalable.
5. The distributed consensus in organizers provides for fault tolerance. For example, a one-node fault tolerant system can be designed using four nodes.
6. Early detection of state machine inconsistencies by executing smart contracts on all the coordinating nodes checks further propagation of nondeterministic transactions into organizing service.
7. Writing policies that limit the number of representatives and coordinators for endorsements and validation may work to improve the transactions' throughput. Higher numbers of requests can be entertained from the clients simultaneously and submitted to the ordering service.

Data like a patient's demography, list of allergies, prescriptions, and sizable documents like MRI, X-rays, endoscopy reports etc. are stored off the chain in traditional systems. The authorized users can access them through secured links.

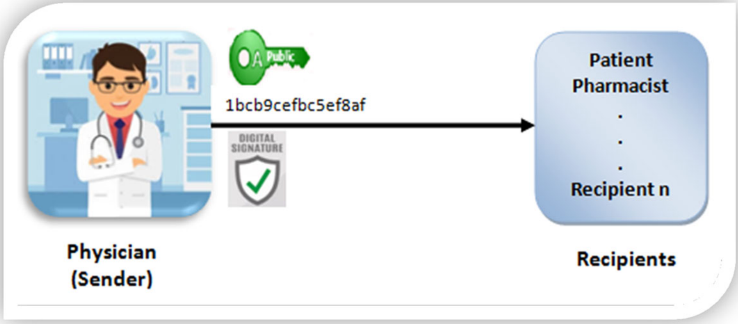

Figure 6. Sample transaction of record between physician and recipients.

The proposed architectural design can accommodate public key cryptography for secure health information exchange (HIE). A transaction showing that a doctor has uploaded a prescription for a patient is sent along with the doctors' signature and a public key of the doctor. A recipient can validate the transaction by verifying the digital signature and computing a hash of the doctor's public key (Figure 6). Such a mechanism provides for complete nonrepudiation by the sender.

5. Implementation and results

The authors tested the proposed system on 14 Windows 10 64 bit PC with 4 GB of RAM and equipped with an Intel 2.4-GHz processor. The 128-bit MD5 hash value was calculated using a crypto module in node.js. The 128-bit hash value is represented using 32 hexadecimal digits. The block was realized using a simple javascript class. Of the 14 nodes, two sets of three nodes were designated as coordinating and representative, respectively. Of the coordinating set, one node was maintaining a local copy of the global ledger. Five nodes among the remaining were assigned the task of ordering service. One node worked as a client and two were committer nodes maintaining the public ledger. Validation at the network nodes is implemented using javascript listening to a transaction on some port. For example, a representative node is implemented as a server listening to some message on port number 7777. A node.js implementation for a representative node is shown through code snippet 1 and code snippet 2 and is available at https://github.com/ratneshlit/Blockchainhealth.

Code Snippet 1: md5module.js

```
var crypto=require('crypto');
exports.md5Hash function (pubKey) {
    return crypto.createHash ('md5'). update (pubKey).digest ('hex');
};
```

Code Snippet 2: representative.js

```
var hash=require(’./ md5module’),
var sys require ("sys"),
my_http require ("http");
my_http.createServer (function(request, response){
    sys.puts ("Proposal Received");
    message request.body.message
    pubKey request.body.patientId
    signature request.body.signature
    source request.body.source
   if (sourcehash.md5Hash(pubKey) && verifySig(signature)){
      var proposal {message:message, flag:’E’}
      request.body.message proposal
      request.redirect (’…/coordinator1’);
      request.redirect (’…/coordinator2’);
      request.redirect (’…/coordinator3’);
    }  else{
       var proposal {message:message, flag:’D’}
       request.body.message proposal
       request.redirect (’…/coordinator1’);
       request.redirect (’…/coordinator2’);
       request.redirect (’…/coordinator3’);
    }
    response.writeHeader (200, {"Content-Type": "text/plain"});
    response.write ("Proposal Received ");
    response.end ();
    }).listen(7777);
```

We performed an analysis over transaction throughput against the number of participating nodes for the proposed blockchain setup. Transaction throughput is defined as the rate at which valid transactions are committed by the blockchain in a predefined time.

We started with a single committer node responsible for updating the public ledger, three endorsing nodes, three representative nodes, and five organizers.

Then we observed the performance of the network throughput in different configurations of the participating nodes, which is reported in Table 1and shown in Figure 7. In Table 1, the same color code explains the set of configurations where the change in a particular parameter is being observed by keeping other parameters constant. The numbers in bold signify the parameter values being changed against the other parameter's value (plaintext) keeping constant for a given set of configuration. “-do-” indicates that the parameter values for the subsequent configurations are constant, only parameters that are written in bold are changing. Note that the throughput is measured in the number of transactions per 5 minutes. We observe that the number of ordering nodes do affect the throughput of the network considerably, while representative, committers, and coordinators affect the network throughput largely due to network latencies. We also observe that, at the minimal load, as large as 16 transactions can be performed.

Table 1. Network throughput in different configurations of the participating nodes.

Config. no.	Representative	Coordinators	Orderers	Committers	Throughput
1	3	3	5	**2**	**5**
2	-do-	-do-	-do-	**1**	**6**
3	3	3	**4**	2	**6**
4	-do-	-do-	**3**	-do-	**7**
5			**2**		**9**
6			**1**		**10**
7	3	**2**	5	2	**6**
8	-do-	**1**	-do-	-do-	**7**
9	**2**	3	5	2	**5**
10	**1**	-do-	-do-	-do-	**5**
11	2	3	**4**	2	**6**
12	-do-	-do-	**3**	-do-	**8**
13			**2**		**9**
14			**1**		**12**
15	1	3	3	**2**	**9**
16	-do-	-do-	-do-	**1**	**9**
17	1	1	1	1	**16**

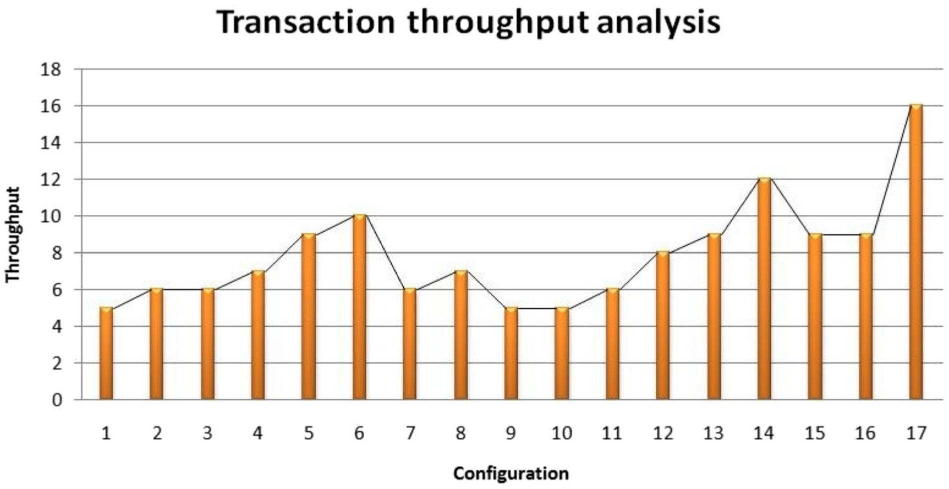

Figure 7. Performance analysis.

6. Conclusion and scope of future work

We propose a secure and transparent mechanism for healthcare-data exchange using a distributed system based on the blockchain. Reports and prescriptions of patients are stored using hash values of the patient ID. An authorized person can only make a transaction to retrieve stored reports. Because blocks in a blockchain do not hold enough space to store heavy-sized reports, we stored such reports on conventional servers. Because the transactions are replicated over multiple nodes, if some nodes are compromised, the data will still be safe. We used the md5 algorithm for generating hash, which could be replaced with SHA-1 or other more efficient algorithms. Multiple representatives, coordinators, and organizers provide for the fault tolerance in the proposed system. For reference, we also provide a node.js implementation of representative nodes.

The future extension to the proposed work lies in streamlining the healthcare business more and more through the blockchain network without violating federal laws. The proposed framework may also be adapted to suit a number of other use cases ranging from trustable courier systems to corruption-intolerant governance (Nakamoto 2009; Melli 2019).

About the authors

Prateek Pandey was born in India in 1983. He has earned his PhD in Computer Science and Engineering in the year 2015. Currently he is an Assistant Professor in the CSE department at Jaypee University of engineering and technology, India. Dr. Pandey has worked in the area of Business Process Management, Software Engineering, and Forecasting. He is an active researcher in the field of machine learning, Blockchain and Elderly care through technological intervention. He has published various research papers in international journals of repute. He has also published an Indian patent for intelligent and adaptive control for micro hydro plant.

Ratnesh Litoriya was born in India in 1983. He received the BTech (Information Technology), ME (Computer Engineering), and PhD (Computer Engineering) degrees from different reputd Universities of India in 2004, 2007, and 2015, respectively. He has been with the department of computer science and engineering, Jaypee University of engineering and technology, India, where he is currently an Assistant Professor. His research interests covers software engineering, machine learning, Fuzzy intelligence, elderly care, Blockchain technology, and their application areas. Dr. Litoriya is a Microsoft certified professional in dot net technology and the recipient of International Award for Professor with Huge Potential in Engineering conferred by World Federation of Science & Technology. He has published various research papers in international journals of repute. He has also published an Indian patent for intelligent and adaptive control for micro hydro plant. He has been on the Editorial Board of several International journals.

References

Ahram, T., A. Sargolzaei, S. Sargolzaei, J. Daniels, and B. Amaba. 2017. Blockchain technology innovations. In Proceedings of the 2017 IEEE Technology Engineering Management Conference (TEMSCON), Santa Clara, CA, USA, June, pp. 137–141.

Alhadhrami, Z., S. Alghfeli, M. Alghfeli, J. A. Abedlla, and K. Shuaib. 2017. Introducing blockchains for healthcare. In Proceedings of the 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA), Ras Al Khaimah, UAE, pp. 1–4. doi:10.1109/ICECTA.2017.8252043.

Angraal, S., H. M. Krumholz, and W. L. Schulz. 2017. Blockchain technology: Applications in healthcare. *Circ. Cardiovasc. Qual. Outcomes* 10 (9):e003800.

Atzori, M. 2015. Blockchain technology and decentralized governance: Is the state still necessary. [Online] Available: https://pdfs.semanticscholar.org/bc1c/abd366fce6d3e1-fe39cd58cf699114d9d13b.pdf

Christidis, K., and M. Devetsikiotis. 2016. Blockchains and smart contracts for the internet of things. *IEEE Access* 4:2292–303. doi:10.1109/ACCESS.2016.2566339.

Conoscenti, M., A. Vetro, and J. C. D. Martin. 2016. Blockchain for the internet of things: A systematic literature review. In Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, Morocco, pp. 1–6. doi:10.1109/AICCSA.2016.7945805.

Dagher, G. G., J. Mohler, M. Milojkovic, and P. B. Marella. 2018. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society* 39:283–97. doi:10.1016/j.scs.2018.02.014.

Engelhardt, M. 2017. Hitching healthcare to the chain: An introduction to blockchain technology in the healthcare sector. *Technology Innovation Management Review* 7 (10):22–34. doi:10.22215/timreview/1111.

Guo, R., H. Shi, Q. Zhao, and D. Zheng. 2018. Secure. *IEEE Access* 6:11676–86. Attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. doi:10.1109/ACCESS.2018.2801266.

IBM Institute for Business Value. 2016. Healthcare rallies for blockchains: Keeping patients at the center [Online]. Available: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03790USEN

Karafiloski, E., and A. Mishev. 2017. Blockchain solutions for big data challenges: A literature review. In Proceedings of the IEEE EUROCON 2017—17th International Conference on Smart Technologies, Ohrid, Macedonia, July, pp. 763–768.

Krawiec, R, and M. White. 2016. Blockchain: Opportunities for health care [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-blockchainopportunities-for-health-care.pdf

Kuo, T. T., H. E. Kim, and L. Ohno-Machado. 2017. Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association* 24 (6):1211–20. doi:10.1093/jamia/ocx068.

Kuo, T. T., H. Zavaleta Rojas, and L. Ohno-Machado. 2019. Comparison of blockchain platforms: A systematic review and healthcare examples. *Journal of the American Medical Informatics Association* 26 (5):462–78. doi:10.1093/jamia/ocy185.

Liu, W., S. S. Zhu, T. Mundie, and U. Krieger. 2017. Advanced block-chain architecture for e-health systems. In Proceedings of the 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom), Dalian, China, pp. 1–6. doi: 10.1109/HealthCom.2017.8210847.

Macdonald, M., L. Liu-Thorrold, and R. Julien. 2017. The blockchain: A comparison of platforms and their uses beyond bitcoin. Working Paper 1–8.

Melli, J. P. 2019. Why is it important to secure your healthcare data from hackers? [Online] Available: https://thecareissue.jaga-me.com/cybersecurity-healthcare/

Mettler, M. 2016. Blockchain technology in healthcare: The revolution starts here. In Proceedings of the 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, Germany, pp. 1–3. doi:10.1109/HealthCom.2016.7749510.

Nakamoto, S. 2009. Bitcoin: A peer-to-peer electronic cash system. Available [Online]: https://bitcoin.org/bitcoin.pdf

Nugent, T., D. Upton, and M. Cimpoesu. 2016. Improving data transparency in clinical trials using blockchain smart contracts. *F1000Research* 5:2541. [Online]. Available: https://f1000research.com/articles/5-2541/v1. doi:10.12688/f1000research.9756.1.

Patel, V. 2018. A frame work for secure and decentralized sharing of medical imaging data via block chain consensus. *Health Inform. Journal* 25 (4):1460458218769699.

Rehman, J. 2017. Difference between centralized, decentralized and distributed processing. [Online] Available: http://www.itrelease.com/2017/11/difference-centralized-decentralized-distributed-processing/

Ristevski, B., and M. Chen. 2018. Big data analytics in medicine and healthcare. *Journal of Integrative Bioinformatics* 15 (3):20170030. doi:10.1515/jib-2017-0030.

Roehrs, A., C. A. da Costa, R. da Rosa Righi, R. Alex, C. A. Costa, and R. R. Righi. 2017. Omni PHR: A distributed architecture model to integrate personal health records. *Journal of Biomedical Informatics* 71:70–81. doi:10.1016/j.jbi.2017.05.012.

Rucker, M. 2018. Will blockchain technology revolutionize health care? [Online] Available: https://www.verywellhealth.com/blockchain-technology-in-health-care-4158528

Sater, S. 2019. Blockchain transforming healthcare data flows. [Online] Available : https://ssrn.com/abstract=3171005 or http://dx.doi.org/10.2139/ssrn.3171005

Schumacher. 2017, "Reinventing healthcare: Towards a global, blockchain-based precision medicine ecosystem" [Online]. Available: https://www.researchgate.net/publication/317936859_Blockchain_Healthcare_-_2017_Strategy_Guide

Snell, E. 2018. Healthcare data privacy, security concerns hinder digital adoption. [Online] Available: https://healthitsecurity.com/news/healthcare-data-privacy-security-concerns-hinder-digital-adoption

Ward, M. J., K. A. Marsolo, and C. M. Froehle. 2014. Applications of business analytics in healthcare. *Business Horizons* 57 (5):571–82. doi:10.1016/j.bushor.2014.06.003.

Yin, S., J. Bao, Y. Zhang, and X. Huang. 2017. M2M security technology of CPS based on blockchains. *Symmetry* 9 (9):193. doi:10.3390/sym9090193.

Yli-Huumo, J., D. Ko, S. Choi, S. Park, and K. Smolander. 2016. Where is current research on blockchain technology?—A systematic review. *PLoS ONE* 11 (10):e0163477. doi:10.1371/journal.pone.0163477.

Zhang, P., D. C. Schmidt, J. White, and G. Lenz. 2018. Blockchain technology use cases in healthcare. In *Advances in Computers*. Amsterdam, Netherlands: Elsevier.

Zheng, Z., S. Xie, H. Dai, X. Chen, and H. Wang. 2017. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Boston, MA, USA, December, pp. 557–564. doi:10.1109/BigDataCongress.2017.85.