Securing Healthcare IoT (HIoT) Monitoring System Using Blockchain

Arsalan Siddiqui
School of Information Technology
Illinois State University
Normal, USA
Asiddi3@ilstu.edu

Dr. Jihad Qaddour
School of Information Technology
Illinois State University
Normal, USA
jqaddou@ilstu.edu

Dr. Sameeh Ullah
School of Information Technology
Illinois State University
Normal, USA
sullah@ilstu.edu

Abstract— **Healthcare IoT (HIoT) is experiencing exponential growth in research and industry, but it still suffers from privacy and security vulnerabilities. Blockchain is distributed immutable ledger without a central authority have been used recently to provide security and privacy in peer-to-peer networks with similar topologies to HIoT. In this paper, we propose a blockchain-based framework for healthcare IoT applications which provides an efficient privacy-preserving access control mechanism and securing the patient sensitive data. This framework combines two robust technologies of our time healthcare IoT (HIoT) and blockchain technology to help creating secure patient diagnosis just like a classical medical report but digitally like an E-health card. Through this model, patients can wear the IoT healthy pi kit device to measure their vitals' information. Then, the flow of patient sensitive data will be secure by applying the blockchain technology. Moreover, we proposed two storage locations off-chain database and IPFS network which will create two points of storage while achieving consistency, integrity, and availability through HIoT blockchain network.**

Keywords-IPFS; blockchain; Arduino; IoT; Healthcare IoT (HIoT); Off-chain database.

I. INTRODUCTION

During such times of crisis as the Covid-19 lingers on and with people experiencing social distancing, Healthcare is in a very precarious state. Doctors are in a lot of stress due working overtime and staying in hospitals due to Covid-19. They must treat Covid-19 patients with serious conditions and also patients with regular day to day conditions. If the general public is given advice on their daily wellbeing, they can easily administer their basic health and only approach the doctors if their health state is worse. Such scenarios has forced researchers to look into avenues which can make life of a doctor easier if people can be given adequate knowledge and advice without having them to show up to the doctor for an appointment and the doctor can focus on patients that are in critical condition. This where IoT devices come in place by relieving the doctors, patients themselves can measure their vitals such as Heartrate, Spo2, Respiration, Temperature, Blood Pressure, Glucose level. Hence, nowadays a lot of IoT devices have sprung up which measure such parameters of a person from the comfort of their home and send the information via cloud to the doctor. As safe as this flow of information may sound, it is actually susceptible to attacks like man in the middle or DDos[40]. These attacks over on the cloud and patient's sensitive information can be retrieved which violates HIPPA regulation [34], the Health Insurance Portability and Accountability Act of 1996 (HIPAA). To counter this problem, our paper proposes a framework with two storage locations and uses IoT sensors which is already available in the market, but we integrate them with the blockchain technology so that patients can securely send data to the relevant parties. Since blockchain technology is immutable that means any tampering in the data is detected as soon as it is done, and that data is discarded, making all the blocks in the chain void. This is because blockchain creates transactional hashes when blockchain is applied to the data. Each block has two hashes, the previous hash of the block and current hash which plays an important role in securing the data.

i. A. Our Contribution

In this paper we proposed and implemented a framework to integrate blockchain with healthcare IoT system using the healthy pi kit. We have also used two storage locations to handle and store patients' sensitive information in the off-chain database and IPFS network for maintaining patient reports and redundancy of the patient's data. The HIoT system will support patients and doctors which will provide real-time 24/7 health monitoring facilities.

ii. B. Organization of the Paper

The remainder of the paper is organized as follows: Section II presents blockchain review. In Section III, we discuss the smart contracts. Section IV discusses blockchain use in cases of health care. In Section V, the healthcare IoT system is introduced. Then, in Section VI, we present IoT integration with blockchain. In Section VII, the proposed model was discussed. In Section VIII, we present the result and discussion. Finally, we conclude the paper with section IX and in Section X proposed a future scope.

II. BLOCKCHAIN

Blockchain is a decentralized, distributed, and digital ledger consisting of records or information called blocks that is used to record transactions across many nodes so that any involved block cannot be altered retroactively, without the alteration of

all subsequent blocks. As data is entered inside the block chain, it is not easy to chain the data. Each block contains data, hash of the current block and hash of the previous block. It uses hashing to check the integrity of the blocks. Each block acts like a smart ledger, can record and update information. There are multiple blocks in a blockchain, and each block stores the hash value of the previous block to validate the integrity of the block. This way it eliminates the need to have a centralized controller hence it is called a decentralized technology. If an attacker tries to exploit or change an information than he has to do that change on all the blocks in a blockchain, even if the information of one block is changed the hash value of that block would change which in turn goes to the next block where the changed hash value would be exposed as fraud. Another reason why it is secure is because all the nodes have the same information in the forms of blocks so whenever a new block is added it is first validated by all members in the network and once it is validated it is entered to the blockchain as a valid block. If somehow data has been tampered in one of the nodes, it surely cannot be done in all the nodes hence that fraudulent data can be caught. That is the reason for using the blockchain technology to secure the HIoT system.

Blockchain came into prominence after being adopted by the famous crypto currency Bitcoin [2]. Transactions are recorded by blocks and stored in a decentralized manner forming a distributed ledger. All the nodes connected have this ledger distributed to them making everyone in the network containing copy of all the transactions. Each block in blockchain contain hash of the previous block. [3] Consensus algorithms are employed to validate the trustworthiness of the blocks. Various types of consensus algorithms are mentioned in Section 3. These algorithms are used to determine which node gets the chance to store and append the next block. Some of the famous Consensus algorithm are Proof of Work (PoW), Proof of Stake (PoS) and Proof of Authority (PoA). Miners are the ones who solve the puzzle first using the consensus algorithms. Figure 1 shows a sample blockchain.

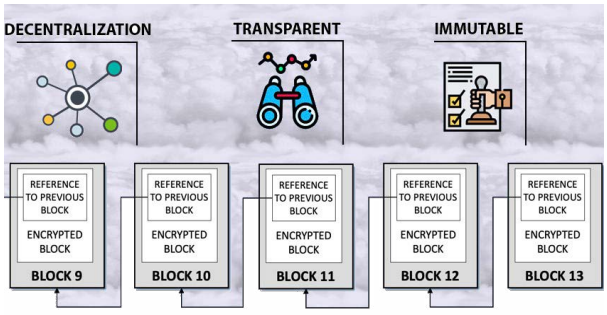

Figure1 Basic Blockchain Structure

A. Proof Of Work (PoW)

One of the popular methods of reaching consensus in block chain is Proof of Work to detect if any tampering is done in any node inside the block chain. The miners compete to solve complex puzzles. Since this hash value is one directional it can only be validated and not be used to trace back the source. Miners guess a random number called the nonce. The nonce is then combined with the block data and passed through hash function gives a hash value which is then broadcasted in the network to other nodes for validation and when the block is verified it is added to the block chain by the miner who solved and in return he receives the block reward [38]. To target a block chain using proof of work lots of computational power as well as time is needed and most of the time the rewards is quite less than the cost of the computational power required to complete the attack. However, a major problem in Proof of work is that since it does so much work by solving the complex puzzles, it requires expensive hardware which consumes large amounts of energy and time. The famous crypto currency Bitcoin uses the proof of work algorithm.

B. Proof of Stake

The first Proof-of-Stakes (PoS) network, Peercoin [35], was developed as a PoS consensus mechanism with the aim to reduce the computational requirements of PoW. Instead of mining the block, in proof of stake the blocks are forged by having a random election process which selects a node to be the validator of the next block. Proof of stake uses transaction fees instead of rewards in proof of work as rewards. In order to be elected to forge the next block the users lock certain amount of coins in the network as part of their stake. The more coins the users have locked the more chance it is for it to forge the block but that's not always the case because PoS uses multiple techniques to make sure the wealthiest users don't always get to forge the blocks. PoS uses methods such as randomize block selection and coin age selection into the election process. In Randomize block chain method those users are selected which have the lowest hash value as well as the highest stake whereas in the coin age method nodes are chosen by how long their tokens have been staked for and once a node is elected their coin age resets and since the election process is public other nodes also gets chance to be elected to forge the next block [36]. When the node no longer wishes to be the forger its stake and rewards are released after a certain period of time to make sure all the information of the block are validated on the network and if a fraudulent block is caught inside the block chain during validation certain part of the stake is lost by the node as well as its ability to be the forger in the election process. This is more secure than the proof of work because in order to approve fraudulent transactions inside a block chain, a node has to own a majority attack on the network known as the 51% attack. Which is not feasible because the stake is more the cost of the attack. Furthermore, the proof of stake is energy efficient as it does not need to solve complex puzzles like in proof of work and more secure and since it does not need expensive equipment it's easy to run nodes. Since there are less needs to release new coins the price of the coins remain stable and it also achieves the main purpose of the blockchain is that it keeps it decentralized by eliminating the need of mining pools which were growing in popularity and sharing more and more coins with each other.

As an example, Ethereum the popular cryptocurrency uses the proof of stack algorithm.

C. *Proof of Authority (PoA)*

Proof of Authority is a modified version of Proof of Stake. This is different from proof of stake in a way that instead of the monetary value of the validator, his identity is more important. This deals with the non-repudiation of the validator that he is who he claims to be which can be tracked through his personal identification on the platform. Two of the Ethereum test networks Kovan and Rinkeby also use PoA to reach consensus. Just like in normal life a person has one identity, this is exactly how PoA operates each validator having one identity. In order to stake his identity, the validator must disclose who he is to get the right to validate the blocks [37]. This voluntary giving away of the identity makes the validators actors in a professional and ethical manner and those whose identities are at stake are tasked in securing and preserving the network. Just like a background check the validators who want to stake their identity must undergo notary exams and attest to clear background. Even getting notary license does not guarantee authority. It just makes staking identity equal for everyone and if the stake is lost unlike PoS it's harder to get it back.

III. SMART CONTRACTS

A smart contract is basically a binding legal document between two parties which states all the rules and regulations both parties have agreed under which they will operate. Nick Szabo in 1990 first proposed the term smart contract [7]. Smart contracts are computer programs which are executed when a predefined condition is triggered. The contents of the smart contract are stored in the blockchain. As opposed to the regular contracts, smart contract does not need third party validation for the predefined conditions to be met, neither it must wait for long time or bear extra cost for the triggering of the event. Hence combining blockchain with smart contracts make a truly immutable system. In case of blockchain based smart contracts, contracts are nothing but scripts residing on the blockchain, which can execute them. One can trigger a transaction to a smart contract by using the unique addresses assigned to it by the blockchain technology [8]. Figure 2 shows basic structure of a smart contract. The most prominent smart contract is Ethereum [12]. Ethereum is designed based on Turing programming language, that permits the meaning of smart contract and decentralized applications. The code in Ethereum's agreements is written in "Ethereum virtual machine code", a low-level, stack-based bytecode language. As often as possible, smart contracts require access to information about real-world states and events. These entities are critical for the effective incorporation of smart contracts inside this present reality, yet they likewise make greater unpredictability, since validation, security, and trust in oracles must be given that bring new energizing difficulties. Appointing contract execution to PCs carries with it a few issues, since it makes them defenseless against specialized issues, for example, hacking, bugs, infections, or correspondence disappointments. Bugs in agreement coding are particularly basic due to the irreversibly and permanent nature of the framework. The advantages of smart contracts do not come without a cost, as they are vulnerable to a series of attacks [10] and [11].

Figure 2 Smart Contract Structure.

IV. BLOCKCHAIN USE CASES IN HEALTHCARE

In this section, we center around the main examinations grouped by a few use cases, for example, electronic clinical records, pharmaceutical supply chain and medical coverage claims.

A. *Electronic Healthcare Records (EHR)*

Electronic Healthcare Records (EHR) can benefit a lot from the blockchain infrastructure. [23,24]. These EHR records contain patient information as well as their medical history, projects about their health, if any progress is made during the treatment. Having the EHR on blockchain makes them public which removes the obstacles of having a centralized source controlling the data and makes the information easily verifiable. The patient will be more at ease and share his records with any 3rd party affiliates like doctors, pharmacists, insurance companies giving them security and privacy [25], [26].

B. *Pharmaceutical Supply Chain*

Pharmaceutical industry is another use case in healthcare where blockchain can be efficiently put into good use. Blockchain address can address a lot of issues pharmaceutical supply chain some of those implementations are mentioned in this paper. The issue of counterfeit drugs have been mentioned in [8,9] where the authors have proposed a model system which can trace pharmaceutical supply of drug end to end to end.Modium.io AG [4] is startup which controls the temperature requirements of each individual drug during transportation, they do this by creating access to the temperature records to the involved party using blockchain Jamil et al [15] in his paper has proposed a solution which helps in detecting counterfeit drugs to combat drugs falsification.

C. *Health Insurance Claims*

Another beneficiary of the immutability nature of the blockchain network is the health insurance industry. This is one of those sectors in the healthcare industry which can benefit a lot because health insurance claims need to be validated by the insurance company before granting it to the insurer, however, there have been very limited implementations in this area. MIStore [27] is one of such implementations which provide storage to the medical insurance data through blockchain.

V. HEALTHCARE INTERNET OF THINGS (HIOT)

In Traditional healthcare system patient was only able to communicate with doctor through visits and tele health services. Internet of Things devices made it possible for doctors to monitor patient's health remotely [41]. This increased patient engagement and helped doctors to give patients care, including remotely.

A. IoT for Patients:
Patients can wear IoT wearable device like the one in our implementation. It can give real time measurements of the patients so immediate care be given to the patients [41].

B. IoT for Physicians:
Data from the IoT devices can help physicians track patient's data which can help them in treating the patients in the longer run as it helps them to identify best treatment process for their patients [41].

C. IoT for Hospitals:
Hospitals can not only use IoT devices for the patients but can also use them to track their various inventories at various locations. It can also help them in maintain temperature of certain rooms for patient care or to place medicines [41].

VI. IOT INTEGRATION WITH BLOCKCHAIN

The IoT is changing and enhancing manual cycles to make them some portion of the computerized time, getting volumes of information that gives information at incomprehensible levels. During the most recent couple of years, distributed computing advances have added to give IoT the essential usefulness to break down and measure data and transform it into continuous activities and information. Concentrated models like the one utilized in distributed computing have added to the advancement of IoT. The mix of promising advances like IoT and distributed computing has demonstrated to be important. We recognize the gigantic capability of blockchain in reforming the IoT. Blockchain can improve the IoT by offering a confidence in sharing assistance, where data is solid and can be discernible. The utilization of blockchain can supplement the IoT with dependable and secure data. IoT can significantly profit and be more secure by the integration of blockchain with IoT technology, which will assist in creating many IoT secured advancements applications. Blockchain innovations will give conceivably advances to different IoT protection and security issues. Some of the integration improvements to HIoT system are:

A. Decentralization and Adaptability
The migration towards a P2P system will present problems such as bottlenecks and centralized failures removed from the equation. The decentralization will help in scalability, fault tolerance of IoT devices and data. The decentralization will also prevent certain authority organizations to control the flow of information.

B. Identity:
Utilizing a common blockchain framework, members can distinguish every device connected to the network. Data once provided to the network cannot be changed due the immutable nature of blockchain. Blockchain can also securely authenticate IoT applications [28]. This would overall be an improvement in the IoT field.

C. Autonomy
With blockchain the future of next generation applications is bright as they support the development of smart autonomous assets and hardware as a service. [29,30] The decentralized nature of blockchain allows them to communicate with each other without any servers.

D. *Reliability*
Blockchain (BC) IoT data becomes immutable over time [31] The validators in the blockchain system makes sure data is not tampered with and every block is validated before being appended in the chain. This in turn brings dependency and reliability in the IoT through blockchain.

E. Security:
As data in blockchain is stored as transactions, current protocols regarding the handling of data in IoT can be immensely secured [32].

VII. PROPOSED MODEL

We propose a blockchain-based framework for healthcare IoT (HIoT) applications, which provides an efficient privacy-preserving access control mechanism and securing the patients sensitive data. This framework combines two robust technologies of our time healthcare IoT (HIoT) and blockchain technology to help creating secure patient's diagnosis just like a classical medical report but digitally like an e-health card. Through this model, patients can wear the IoT healthy pi kit device to measure their vitals' information. Then, patient sensitive data will be secure by applying the blockchain technology. Figure 3 shows the system architecture of our proposed model where we use Hyperledger Fabric blockchain technology, detail is in subsection A, which is applied directly at the IoT sensor's data measurement. As shown in the figure 3, two secured copies flow from the blockchain, one sent to cloud database and redundant copy of the same patient's data will be send to Inter planetary file system (IPFS) for more security and redundant of the patient's data as a secured second copy. Doctor can access the data through website or a mobile apps.

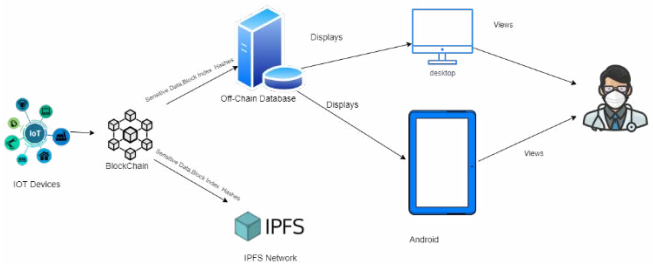

Figure 3 IoT devices and Blockchain storage

The processes involved are as follow:

A. Blockchain Hyperledger Fabric

Hyperledger Fabric (HF) is a product of the Linux Foundation's Hyperledger Project. HF was developed in March 2016 from a combination of several existing initiatives, including IBM's open blockchain, Digital Asset's Hyperledger, and block stream's libconsensus. Of the various products available from the Hyperledger Project, Hyperledger Fabric has become the most successful to date. It is being utilized in production environments in more than twenty companies around the world, including IBM and Oracle.

Hyperledger Fabric is a permissioned-only, or private-only, distributed ledger. All nodes participating in its network require permission from the hosting organization. Permission is granted via a public key infrastructure (PKI) using either a Hyperledger Fabric certificate authority (CA) or a public CA. This permission usually takes the form of an X.509 digital certificate, but other forms of verification can be used, although, HF does not support RSA keys [42]. One feature of HF is the use of communication channels. Channels provide separation of transactions within the network, granting privacy based on who is allowed on that transaction's channel. They function like virtual local area networks (VLANs). Communication only occurs between nodes which are part of the channel, and membership to a channel must be granted by that channel's controlling organization [42].

B. *IoT Device*

For our project's implementation, we have used Healthy pi kit [22]. This kit comes embedded with four sensors and measure these parameters in real time with high accuracy. These sensors are Electrocardiogram (ECG) data, heart rate, and heart-rate variability, respiration based on impedance pneumography, pulse oximetry (SPO_2) and body temperature. Figure 5 shows the healthy pi kit IoT device. This real time data passes through our blockchain network and creates transactions which creates secure immutable records. These sensitive records are then saved into an off-chain database.

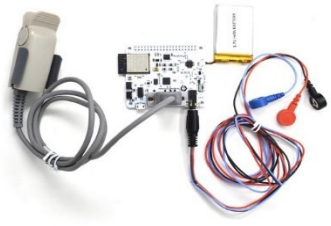

Figure 4 Healthy pit kit device

C. *Off-Chain Database*

It is the information base where the basic boundaries of the body and different records of patients are put away. The shrewd agreement controls admittance to this information base. Perusing or composing procedure on this information base depend on the rights the situation director awards to the clients. Information base level assurance measures are utilized to guarantee protection and uprightness of information. Alternatively, information can be hashed to the information base prior to being put away.

D. *Inter planetary file system (IPFS)*

IPFS is a protocol designed to store decentralized and shared files enabling a P2P distributed file system to make the web safer, faster and more open. IPFS is intended to increase the efficiency of the web at the same time as it removes duplication and tracks version history for each file [18], Hence in order keep a redundant storage option. The patient vital information is also stored by a peer in IPFS. That storing results in the IPFS creating a content-based hash which can be decrypted to view the patients vital.

E. *Doctor*

A Doctor can verily access the application and get access to patients' vital information. The blockchain is designed in such a way that only authorized doctors can see patient's vital data through the frontend applications through web or mobile apps.

VIII. Results and Discussion

As mentioned in our proposed model. When a wearer wears the healthy pi kit. The kit takes measurement of the parameters that it is designed to take which passes through our API to our blockchain in real time. The blockchain is applied to the data coming from the sensors and creates hashes and other parameters. The block constantly gets validated by the chain to see if there is any discrepancy. Figure 5 shows a flowchart which explains the flow of data from the sensors to the storage. Figure 6 shows the Json format for the blockchain which contains all the blocks that have been mined. That json load is displayed into the URL using flask application and all those blocks are in real time measurements of the wearer of the healthy pi kit. That json load then with the help of an API is stored in the Off-chain database then it is displayed into the frontend through website or mobile apps.

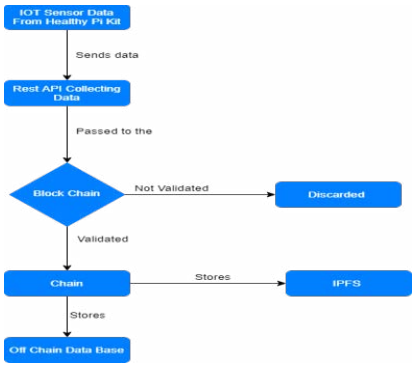

Figure 5 Flow of IoT Data

Figure 7 shows the blockchain displayed in the frontend with each blocked mine separately but forming a chain. The values shown are just for demonstration purposes final version will not have the sensor measurements there. Another copy of the blockchain gets uploaded into the IPFS networks where individual nodes in that network store the sensitive patient information.

Figure 6 Blocks in json Format

ID	Temperature	Heartrate	Respiration	Spo2	Timestamp	Block	Proof	PreviousHash
1	85	0	-999	29.96	2020-12-09 03:39:35	2	533	458f96710709aaa68389e1590c5bdbbd304d538edcd667da4f8ccfa4a4655028
2	119	0	-999	29.82	2020-12-09 03:41:50	3	45293	ca6cd9f6ecc1ba359a805e2dd0d6183b204ece3dc9432faedbed7d5461c151c9

Figure 7 Blocks in Frontend application

IX. CONCLUSION

In this paper we have presented a framework to implement and integrate blockchain with healthcare IoT system and the healthy pi kit. We have also used two storage locations to handle and store the sensitive patient information in the off-chain database and IPFS network for maintaining patient reports and redundancy of the patient's data. Our reasoning behind having two separate storage location to get redundancy and remove single point of failure. This IoT data works well in blockchain with our framework providing much needed security and privacy to the real time data coming from the health pi kit device

X. FUTURE SCOPE

The Use Cases discussed in section IV can work well if integrated with our model. All those use cases are relevant and the integration of those uses case with our model can create a one window experience for the patient. It will no longer has to coordinate with 3rd parties as the patient can share real time records with pharmacists, insurance and any doctor as long as they agree to the smart contract. Since other parties will join the model smart contract would be generated which should be agreeable by all the parties. Integration of our model with the health insurance claim also makes it easy for them to track and verify patient's data, since our measurements are in real time, they don't have to worry about outdated data being presented to them. Our future scope will really revolutionize the medical industry as blockchain solves many of their problems regarding security, trust, privacy, ease of access to data and no centralized authority.

CRONYMS

API	Application Programming Interface
CA	Certificate Authority
D-DOS	Distributed Denial of Service
ECG	Electrocardiogram
E-Health Card	Electronic Health Card
EHR	Electronic Health Record
HF	Hyper Ledger
HIOT	HealthCare Internet of Things
HIPPA	Health Insurance Portability and Accountability Act
IBM	International Business Machines
IOT	Internet of Things
JSON	JavaScript Object Notation
PC	Personal Computer
PKI	Public Key Infrastructure
POA	Proof of Authority
POS	Proof of Stake
POW	Proof of Work
RSA	Rivest Shamir Adleman
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network

REFERENCES

[1] https://www.prnewswire.com/news-releases/top-cyber-security-experts-report-4-000-cyber-attacks-a-day-since-covid-19-pandemic-301110157.html#:~:text=Microsoft%20reports%20that%20COVID%2D19,day%20in%20the%20U.S.%20alo

[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system,"

[3] https://www.researchgate.net/publication/328686723_Towards_Secure_IoT_Communication_with_Smart_Contracts_in_a_Blockchain_Infrastructure

[4] Bocek, T., Rodrigues, B.B., Strasser, T., Stiller, B.: Blockchains everywhere - a use-case of blockchains in the pharma supply-chain. In: IFIP/IEEE Symposium on Integrated Network and Service Management (IM), pp. 772–777, May 2017

[5] Miguel Castro, Barbara Liskov, et al. Practical byzantine fault tolerance. In OSDI, volume 99, pages 173–186, 1999.

[6] Sunny King and Scott Nadal. Ppcoin: Peer-to-peer crypto-currency

[7] with proof-of-stake. Self-Published Paper, August, 19, 2012.

[8] Bryatov, S., Borodinov, A.: Blockchain technology in the pharmaceutical supply chain: researching a business model based on hyperledger fabric. In: International Conference on Information Technology and Nanotechnology (ITNT), Samara, Russia (2019)

[9] Haq I, Esuka OM. Blockchain technology inInt. J. Comput. Appl. 2018;975:8887. [Google Scholar]

[10] 20. Raj, R., Rai, N., Agarwal, S.: Anticounterfeiting in pharmaceutical supply chain by establishing proof of ownership. In: TENCON 2019–2019 IEEE Region 10 Conference (TENCON), pp. 1572–1577. IEEE (2019)

[11] Nick Szabo. The idea of smart contracts. Nick Szabo's Papers and

[12] F. Zhang, E. Cecchetti, K. Croman, A. Juels, E. Shi, Town crier: an authenticated data feed for smart contracts, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, ACM, 2016, pp. 270–282.

[13] K. Delmolino, M. Arnett, A. Kosba, A. Miller, E. Shi, Step by step towards creating a safe smart contract: lessons and insights from a cryptocurrency lab, A. Reyna et al. / Future Generation Computer Systems 88 (2018) 173–190 189 in: International Conference on Financial Cryptography and Data Security, Christ Church, Barbados, Springer, 2016, pp. 79–94.

[14] N. Atzei, M. Bartoletti, T. Cimoli, A survey of attacks on ethereum smart contracts (sok), in: International Conference on Principles of Security and Trust, Uppsala, Sweden, Springer, 2017, pp. 164–186. [48] K. Christidis, M. Devetsikiotis, Blockchains and smart contracts for the internet of things, IEEE Access 4 (2016) 2292–2303.

[15] Jamil F, Hang L, Kim K, Kim D. A novel medical blockchain model for drug supply chain integrity management in a smart hospital. Electronics. 2019;8(5):505. doi: 10.3390/electronics8050505. [CrossRef] [Google Scholar]

[16] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, A. Hobor, Making smart contracts smarter, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, ACM, 2016, pp. 254–269.

[17] V. Buterin, Ethereum white paper, 2013. Available online: https://github. com/ethereum/wiki/wiki/White-Paper (Accessed 2 April 2018).

[18] https://www.researchgate.net/publication/328581609_An_Overview_of_Smart_Contract_and_Use_Cases_in_Blockchain_Technologyhttps://pure.qub.ac.uk/ws/files/144448878/CommsMag_Final.pdf

[19] https://www.perkinscoie.com/images/content/1/6/v2/164979/Smart-Contracts-12-Use-Cases-for-Business-Beyond.pdf

[20] https://www.hhs.gov/hipaa/index.htmlProc. OTM Conf. Move to Meaningful Internet Systems, 2013.)

[21] https://eprints.cs.univie.ac.at/5433/7/sanerws18iwbose main-id1-p-380f58e-35576-preprint.pdf

[22] https://healthypi.protocentral.com/

[23] Medical record system using blockchain, big data and tokenization. In: Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 9977 LNCS, pp. 254–261.

[24] introduction to the blockchain and its implications for libraries and medicine Med. Ref. Services Q., 36 (3) (2017), pp. 273-279

[25] MedRec: Using blockchain for medical data access and permission management Proceedings – 2016 2nd International Conference on Open and Big Data, OBD 2016 (2016), pp. 25-30

[26] Young, Ernst, 2016. Blockchain in health. How distributed ledgers can improve provider data management and support interoperability, Report.

[27] Zhou L, Wang L, Sun Y. MIStore: a blockchain-based medical insurance storage system. J. Med. Syst. 2018;42(8):149. doi: 10.1007/s10916-018-0996-4. [PMC free article] [PubMed] [CrossRef] [Google Scholar]

[28] Gan S.An IoT Simulator in NS3 and a Key-Based Authentication Architecture for IoT Devices using BlockchainIndian Institute of Technology Kanpur (2017)

[29] Chain of things, 2017. Available online: https://www.blockchainofthings.com/. (Accessed 1 February 2018).

[30] Filament, 2017. Available online: https://filament.com/. (Accessed 1 February 2018).

[31] modum, 2017. Available online: https://modum.io/. (Accessed 1 February 2018).

[32] G. Prisco, Slock. It to introduce smart locks linked to smart ethereum contracts, decentralize the sharing economy, 2016. Available online: https://bitcoinmagazine.com/articles/slock-it-to-introduce-smart-locks-linked-to-smart-ethereum-contracts-decentralize-the-sharing-economy-1446746719/.(Accessed 1 February 2018).

[33] Khan M.A., Salah K.Iot security: review, blockchain solutions, and open challengesFuture Gener. Comput. Syst. (2017)

[34] https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

[35] S. King and S. Nadal, PPCoin: Peer-to-peer crypto-currency with proof-of-stake, Self-Published Paper, Aug. 2012,

[36] C. T. Nguyen, D. T. Hoang, D. N. Nguyen, D. Niyato, H. T. Nguyen and E. Dutkiewicz, "Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities," in IEEE Access, vol. 7, pp. 85727-85745, 2019, doi: 10.1109/ACCESS.2019.2925010

[37] https://apla.readthedocs.io/en/latest/concepts/consensus.html

[38] Gervais Arthur, "On the Security and Performance of Proof of Work Blockchains", *CCS'16 Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016.

[39] A. Gervais, H. Ritzdorf, G. O. Karame and S. Capkun, "Tampering with the Delivery of Blocks and Transactions in Bitcoin", *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur. - CCS '15*, pp. 692-705, 2015.

[40] https://us-cert.cisa.gov/ncas/tips/ST04-015

[41] https://www.wipro.com/en-US/business-process/what-can-iot-do-for-healthcare-/#:~:text=IoT%20explores%20new%20dimensions%20of,opportunities%20and%20improving%20healthcare%20operations.

[42] Hyperledger Fabric Documentation, "A blockchain platform for the enterprise," Hyperledger Fabric release 1.4.3, 2019. Retrieved from https://hyperledger-fabric.readthedocs.io/en/release-1.4/. Last accessed: October 14, 2019.