A Hyperledger Fabric-based Blockchain Architecture to Secure IoT-based Health Monitoring Systems

Filippos Pelekoudas Oikonomou
Instituto de Telecomunicações
Aveiro, Portugal
Faculty of Engineering and Science, University of Greenwich
Chatham Maritime, UK
f.pelekoudas@av.it.pt

Joaquim Manuel C.S. Bastos
Instituto de Telecomunicações
Aveiro, Portugal
jbastos@av.it.pt

Jose Ribeiro
Instituto de Telecomunicações
Aveiro, Portugal
jcarlosvgr@av.it.pt

Jonathan Rodriguez
Instituto de Telecomunicações
Aveiro, Portugal
Faculty of Computing, Engineering and Science, University of South Wales
Pontypridd, UK
jonathan@av.it.pt

Georgios Mantas
Instituto de Telecomunicações
Aveiro, Portugal
Faculty of Engineering and Science, University of Greenwich
Chatham Maritime, UK
gimantas@av.it.pt

***Abstract*—Although blockchain is a promising technology that can bring significant benefits into current centralized IoT-based health monitoring systems in order to address security challenges, the resource-constrained IoT devices of these systems cannot afford complex and heavyweight operations due to their limited processing power, storage capacity, and battery life. Therefore, in this paper, we propose a Hyperledger Fabric-based blockchain architecture to: i) enhance security in IoT-based health monitoring systems, ii) achieve better storage handling due to the limited storage capacity of sensors and gateways, iii) facilitate decentralized accountability, and iv) eliminate single point of failure.**

Keywords— IoT, security, blockchain, healthcare, Hyperledger

I. INTRODUCTION

Over the past few years, we have witnessed the emergence of the Internet of Things (IoT) technology that brings significant benefits to the healthcare sector and can play a noteworthy role in improving citizens' quality of life by enabling IoT-based health monitoring systems that provide personalised healthcare services without time and location constraints [1], [2]. However, the wide range of different communication technologies (e.g., WLANs, Bluetooth, Zigbee, WANs) and types of IoT devices (e.g., medical sensors, diagnostic tools, wireless access points) incorporated in IoT-based health monitoring systems as well as the fact that the transmission of sensitive healthcare information (e.g., patient's vital signs), between patients and healthcare providers, is done through the Internet are factors that raise many security challenges [3],[4].

Thus, security solutions that meet the fundamental security requirements (i.e., authentication, authorization/access control, data integrity, data confidentiality, and availability) for the ever-evolving IoT-based health monitoring systems are essential for the acceptance and wide adoption of such systems in the coming next years [5], [6]. Nevertheless, the high resource requirements, in terms of computational cost and energy consumption, of complex and heavyweight conventional security mechanisms, cannot be afforded by resource-constrained Internet of Medical Things nodes (e.g., medical sensors) which constitute main components of IoT-based health monitoring systems [7], [8]. Moreover, the centralization approach adopted by the state-of-the-art traditional security frameworks is not well applicable to IoT-based health monitoring systems due to single point of failure issues [7], [9],[10]. In addition, it is worthwhile to mention that conventional defense mechanisms cannot ensure complete tamper proof systems [4].

Therefore, there is an urgent need for novel security mechanisms to address the pressing security challenges of IoT-based health monitoring systems in an effective and efficient manner before they gain the trust of all involved stakeholders and reach their full potential in the healthcare market [3], [4]. Towards this direction, the focus of our research work is on the integration of blockchain technology into novel security solutions for IoT-based health monitoring systems as blockchain has been foreseen by industry and research community as a disruptive technology that can play a significant role in: a) securing IoT devices, which are key elements of IoT-based health monitoring systems; and b) resisting unauthorised access during data transmission (i.e., tamper proof transmission of medical data) [4], [11]. However, despite the significant benefits that blockchain technology can bring into current centralized IoT-based health monitoring systems in order to address their security challenges, the resource-constrained IoT devices of these systems cannot afford complex and heavyweight operations (e.g., mining process in Proof of Work (PoW)) due to their limited processing power, storage capacity, and battery life [12], [13]. Therefore, in this paper, we propose a Hyperledger Fabric (HLF)-based blockchain architecture to: i) secure IoT-based health monitoring systems, ii) achieve better storage handling due to the limited storage capacity of sensors and gateways, iii) facilitate decentralized accountability, and iv) eliminate single point of failure. It is

worthwhile to mention that we adopted the Hyperledger Fabric blockchain platform as it is a permissioned blockchain platform and presents low processing complexity which are essential characteristics for IoT-based health monitoring systems[12], [13].

Following the introduction, this paper is organized as follows. In section II, we review several blockchain-based architectures for IoT systems. In section III we present the Perception Domain of an IoT-based health monitoring system in which the proposed Hyperledger Fabric-based blockchain is applied. In section IV, the architecture of the proposed Hyperledger Fabric-based blockchain is provided along with details about the main architecture components. Finally, section V concludes this paper.

II. Related Work

In this section, an overview of blockchain-based architectures for IoT systems is given.

A. Dorri et al. in [14] set a milestone for the integration of the blockchain technology with IoT. The concept of Proof of Work (PoW) is eliminated and the need of coins as well. The concepts of local Blockchain and local miner are introduced, and they are being used also in this paper for our proposed scheme. After the publication of Hyperledger Fabric, an open-source system for deploying and operating permissioned blockchains [15], many papers have been based on the implementation of [14] enhancing it with this latest technology.

O. Attia et al. in [16] have focused on this integration of Blockchain and IoT. As in the case of [14], the concept of PoW has been eliminated along with the need of rewards. The proposed framework is focused on the distributed technology as a security mechanism making it more suitable for the requirements of an IoT network. The term of Medical Devices Blockchain is introduced as a mechanism to ensure trust between a network of IoT medical devices.

A. D. Dwivedi et al. in [17] focus on Remote Patient Monitoring (RPM) and introduce a privacy preserving scheme to overcome the restrictions of Blockchain implementation in IoT (high power consumption, slow transaction rate, etc) and exploit its benefits. The authors succeed in decentralization with the use of an overlay decentralised network, they introduce a lightweight ring signature scheme and digital signatures for anonymity of the users and authentication of data, and they adopt the elimination of PoW to achieve scalability.

Furthermore, A. D. Dwivedi et al. in [18] propose a security scheme with the integration of Blockchain in healthcare applications. The IoT networks are arranged in clusters and each cluster elects a cluster head to avoid delays and to reduce overhead in nodes. In correlation with [17], the authors extent the concept of the overlay network, propose the ideas of the transmission of data *"when necessary"* and the storage of the hash in the local blockchain and the healthcare data in the Cloud. Again, in corelation with other proposed works, the authors make use of other algorithms for the validation process over PoW, such as Proof of Authority algorithms which are characterized as algorithms with increased performance in comparison to the typical Byzantine Fault Tolerance Algorithms.

The authors in [19], use Hyperledger Fabric to create a permissioned Blockchain for IoT. The scheme is provided with a certification authority for the registration process and with a local peer structure to interact with an associated anchor peer in the global network. The issues that this work addresses are the transactions per second (TPS) and the limits in the storage requirements of each peer. Each group of IoT devices has a peer for validating the transactions (namely Lpeer). Lpeer works for the organizational IoT devices and in case it is necessary it can be divided into many instances to create a distributed local network to avoid the issue of single point of failure.

H. H. Pajooh et al. in [13] propose and evaluate a more complete blockchain implementation with the use of the Hyperledger Fabric platform. They present a solution for a model introduced in [20] where they create a Multi-layer Blockchain Network for IoT with Local Blockchains that connect different gateways of IoT systems with a Base Station and with a Global Blockchain that interconnects multiple Base Stations. They implement their solution with the use of RPi devices and Virtual Machines and evaluate its performance.

The authors in [19], [16], and [18] note the significance of the implementation of smart contracts in an IoT network. Smart contract is a piece of code embedded in a blockchain that functions as a regulator in order for the transactions to be performed under specific rules, terms, and conditions. In the case of Hyperledger Fabric, used in [19] and [16], smart contracts are replaced with Chaincode, which is the equivalent to smart contracts in the Hyperledger Fabric platform [15].

III. Scenario Architecture

The proposed Hyperledger Fabric-based blockchain architecture is designed for the Perception Domain (i.e., IoT edge network) of IoT-based health monitoring systems, as shown in Figure 1. The Perception Domain of an IoT-based health monitoring system interacts with objects (e.g., physical things) through the IoT devices (e.g., sensors, actuators, etc.) of the IoT edge network. The main purpose of this domain is to connect things into IoT edge network, and to measure, gather and handle the information provided by these things (e.g., patient's body, patient's home environment) through IoT devices (e.g., sensors). Afterwards, the Gateway is responsible to transmit the gathered information outside the Perception Domain (i.e., telecommunication network, Cloud). Finally, the Perception Domain contains the bio-sensors responsible to gather the vital signs of the user-patient (e.g., blood pressure, body temperature, electrocardiogram) and the context-aware

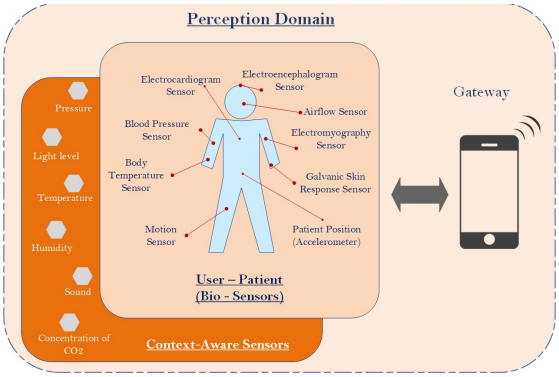

Fig. 1 System Model - Perception Domain

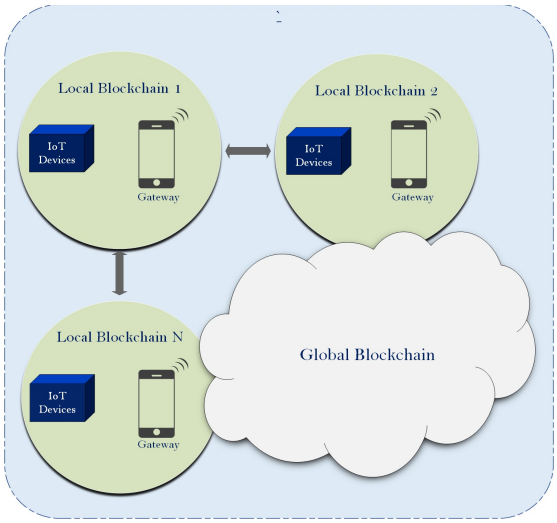

Fig. 2 Proposed Hyperledger Fabric-based Blockchain Architecture

sensors for collecting context information from the user-patient environment (e.g., air pressure, humidity, sound, etc.) as shown in Figure 1.

IV. Proposed Hyperledger Fabric-based Blockchain Architecture

The proposed Hyperledger Fabric-based blockchain architecture consists of: i) a Local Blockchain (LB) for each Perception Domain of each IoT-based health monitoring system, and ii) a Global Blockchain (GB) interconnecting the Local Blockchains of the Perception Domains, as shown in Figure 2.

A. Local Blockchain

The LB of each Perception Domain is responsible to secure the transactions (i.e., communication between devices) taking place into the given Perception Domain. The transactions are initiated by the sensors of the Perception Domain.

To enable the LB of each Perception Domain, we introduce a stand-alone All-in-One component that integrates within the Gateway two sub-components; one that functions as the endorsing-validation *Peer* and another that functions as the *Orderer*, as shown in Figure 3. In other words, the consensus, consisting of the execution-endorsement, ordering, and validation steps, is performed with use of consensus algorithms and after the transactions have been ordered and fulfilled certain criteria in the proposed All-in-One component. Thus, an LB is created inside the Perception Domain by a Peer endorsing-validating the transactions and an Orderer responsible for taking the validated transactions, creating blocks and sending them to the Peer (i.e., committing Peer) to update the Local Ledger in the LB.

In particular, as shown in Figure 3, the *Peer* consists of the following:

- *Endorser-Validator:* it is used to endorse and validate transactions. To endorse, it runs the smart contract (i.e., implemented chaincode) that is related with each transaction and sends the signed outcome to the Orderer. The endorsement from a sole peer is set by the endorsing policies that are included in it. The validation process confirms the transactions that are legit and then the block of transactions is committed to the ledger, which gets updated [21].
- *Chaincode:* also known as smart contract, is a set of rules running during the execution phase in the *Peer* and regulates the transactions in an LB. Chaincode, in Hyperledger Fabric, can be written in Go, Node.js or Java, through a contract interface [15].
- *Ledger:* a tamper-proof database that stores the transactions. The gateway, through the peer, has permission to read/write on the ledger. Ledger data cannot be altered or deleted. It can be separated in two entities, Global and Local Ledger, which will be analysed in the following section.

On the other hand, the *Orderer* functions as the ordering service of an LB. It receives the validated transactions, and orders them according to the reliance that was defined in the execution phase. Then gathers these transactions into a block and produces a hash-chained series of blocks as an output.

Furthermore, due to the significant volume of blockchain data generated in a LB and, at the same time, the limited storage capabilities of Gateways, the issue of data storage in LB is of high importance. In this regard, we propose the following two approaches in order to address this issue sufficiently.

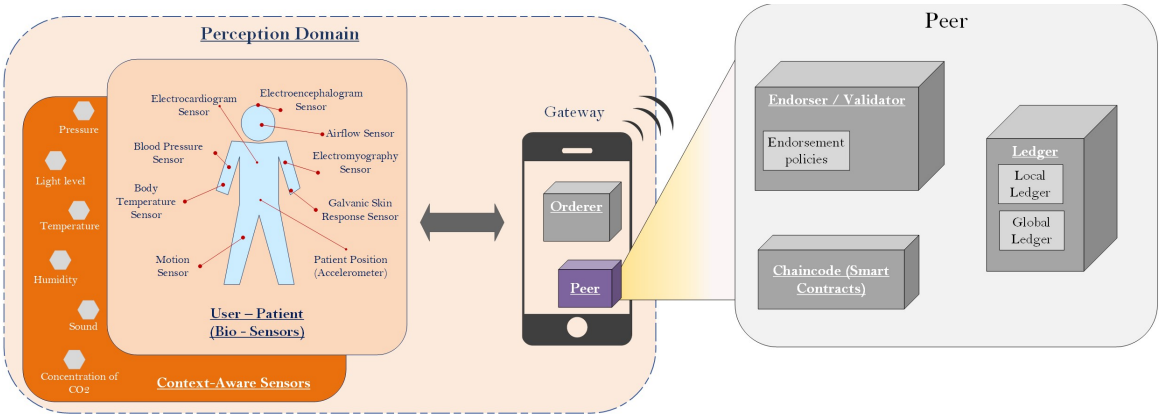

Fig. 3 Gateway Architecture of a Local Blockchain

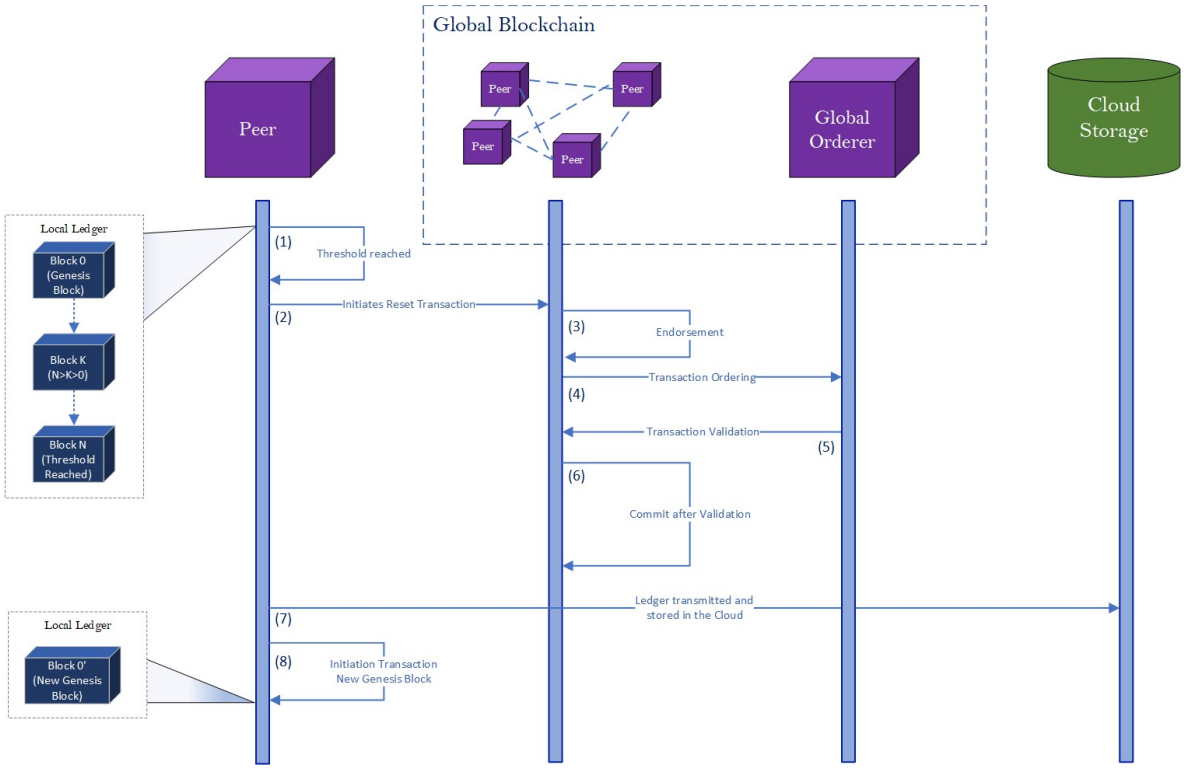

Fig. 4 Sequence diagram of the Reset Transaction

Firstly, we propose that the data collected from the sensors not to be stored inside blocks. Blocks should store only the ID of the sensors involved in each transaction and the details of transaction itself, rather than the actual sensing data, which should be hashed and then pass, through the Gateway to the Cloud where they will be stored. The hash of the data is stored in the blocks to ensure the integrity of the sent data. This way, the Peer of each LB keeps stored in its ledger only the id of the sensors involved in each transaction and the details of transaction itself, which are the minimum data required for ensuring the integrity of the transactions.

Secondly, we also introduce the novel concept of the Reset of LB, as shown in Figure 4. After a certain threshold (1) (i.e., a certain amount of time or a certain size of stored data), the Peer inside the Gateway initiates a Reset transaction (2). The Peer makes a Reset transaction proposal to move the data of the ledger of the LB outside its storage device and free storage space. The transaction is then sent for endorsing (3) in the GB network by other Peers and ordered by the Global Orderer (4) and then back for validation (5) in the GB network. After its completion, the transaction is committed and built within a block in the Global blockchain with other transactions (6). This way from an LB of several blocks and a size of a certain number of bytes, we are led to a block (i.e., built in the GB) whose relevant size in the GB ledger is negligible in comparison with the size of an entire Blockchain such as the LB. The data of the LB ledger that was stored in the Peer previously are not stored inside the GB. Instead, a hash is created for the LB and stored in the GB together with the transaction and the ID of the Peer that proposed it. The data of LB along with its hash is stored in the Cloud storage (7), protecting the integrity of the data. As a last step, the Local Ledger gets erased and an initiation transaction is proposed generating a genesis block (8) for a new LB and validating anew the nodes of the Perception Domain. Although the increase in the number of message exchanges, the Reset Transaction reduces the block storage complexity while the security level increases.

B. Global Blockchain

The GB interconnects the LBs of the various Perception Domains in order to: i) relieve their Gateways (i.e., better storage handling), which have low storage capacity, by storing data to the GB, ii) facilitate decentralized accountability, and iii) eliminate single point of failure, while at the same time ensuring data integrity, availability and accountability at the global level.

Further to the LB for the Perception Domain of an IoT-based health monitoring system, the proposed architecture extends to the creation of a GB with the participation of many *Peers*, located in different Perception Domains, and Cloud servers / databases of health providers. While in an LB each *Peer* acts as an endorsing-validating Peer of the given LB, in the GB each Peer of each LB acts like an endorsing-validating Peer of a larger blockchain (i.e., GB) where a Global Ledger is responsible to store the transactions among the Peers and between the Peers and the Cloud storage. In addition, in the GB, a Global Orderer is located on a trusted server. Finally, the GB runs its own Chaincode and has its own endorsement policies stored inside the Peers as a separate Blockchain.

V. Conclusion and Future Work

In this paper, we proposed a Hyperledger Fabric-based blockchain architecture consisting of: i) an LB for each Perception Domain of each IoT-based health monitoring system, and ii) a GB interconnecting the LBs of the

Perception Domains. The LB of each Perception Domain is responsible to secure the transactions taking place into the given Perception Domain, and the GB aims at i) relieving the resource-constrained Gateways (i.e., better storage handling), ii) facilitating decentralized accountability, and iii) eliminating single point of failure, while at the same time ensuring data integrity, availability, and non-repudiation at the global level. It is noteworthy to highlight that each LB guarantees integrity and tamper-resistance of the sensor ids and transaction details stored in the Local Ledger. On the other hand, the GB ensures integrity and tamper-resistance of the actual sensing data stored in the Global Ledger. Moreover, the tamper-resistance of any LB and the GB ensure non-repudiation. As future work, we intend to implement the proposed architecture in a virtual environment and evaluate it in terms of performance metrics such as transaction throughput, resource consumption, network use and latency.

ACKNOWLEDGMENT

The research work leading to this publication has received funding through the Moore4Medical project under grant agreement H2020-ECSEL-2019-IA-876190 within ECSEL JU in collaboration with the European Union's H2020 Framework Programme (H2020/2014-2020) and Fundação para a Ciência e Tecnologia (ECSEL/0006/2019).

REFERENCES

[1] J. J. P. C. Rodrigues *et al.*, "Enabling Technologies for the Internet of Health Things," *IEEE Access*, 2018, doi: 10.1109/ACCESS.2017.2789329.

[2] M. Papaioannou *et al.*, "A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT)," *Trans. Emerg. Telecommun. Technol.*, 2020, doi: 10.1002/ett.4049.

[3] P. Gope and T. Hwang, "BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network," *IEEE Sens. J.*, 2016, doi: 10.1109/JSEN.2015.2502401.

[4] S. Khezr, M. Moniruzzaman, A. Yassine, and R. Benlamri, "Blockchain technology in healthcare: A comprehensive review and directions for future research," *Appl. Sci.*, 2019, doi: 10.3390/app9091736.

[5] J. Ribeiro, F. B. Saghezchi, G. Mantas, J. Rodriguez, S. J. Shepherd, and R. A. Abd-Alhameed, "An Autonomous Host-Based Intrusion Detection System for Android Mobile Devices," *Mob. Networks Appl.*, vol. 25, no. 1, pp. 164–172, 2020, doi: 10.1007/s11036-019-01220-y.

[6] J. Ribeiro, G. Mantas, F. B. Saghezchi, J. Rodriguez, S. J. Shepherd, and R. A. Abd-Alhameed, "Towards an Autonomous Host-based Intrusion Detection System for Android Mobile Devices," in *Proceedings of the 9th EAI International Conference on Broadband Communications, Networks, and Systems (BROADNETS2018)*, 2018, pp. 139–148.

[7] M. Seliem and K. Elgazzar, "BIoMT: Blockchain for the internet of medical things," 2019, doi: 10.1109/BlackSeaCom.2019.8812784.

[8] J. Ribeiro, F. B. Saghezchi, G. Mantas, J. Rodriguez, and R. A. Abd-Alhameed, "HIDROID: Prototyping a Behavioral Host-Based Intrusion Detection and Prevention System for Android," *IEEE Access*, vol. 8, pp. 23154–23168, 2020, doi: 10.1109/ACCESS.2020.2969626.

[9] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of things: The road ahead," *Computer Networks*. 2015, doi: 10.1016/j.comnet.2014.11.008.

[10] L. Catarinucci *et al.*, "An IoT-Aware Architecture for Smart Healthcare Systems," *IEEE Internet Things J.*, 2015, doi: 10.1109/JIOT.2015.2417684.

[11] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Futur. Gener. Comput. Syst.*, 2018, doi: 10.1016/j.future.2017.11.022.

[12] I. Essop, J. C. Ribeiro, M. Papaioannou, J. Rodriguez, G. Zachos, and G. Mantas, "Generating datasets for anomaly-based intrusion detection systems in iot and industrial iot networks," *Sensors*, vol. 21, no. 4, pp. 1–31, 2021, doi: 10.3390/s21041528.

[13] H. H. Pajooh, M. Rashid, F. Alam, and S. Demidenko, "Hyperledger fabric blockchain for securing the edge internet of things," *Sensors (Switzerland)*, vol. 21, no. 2, pp. 1–29, 2021, doi: 10.3390/s21020359.

[14] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," *2017 IEEE Int. Conf. Pervasive Comput. Commun. Work. PerCom Work. 2017*, pp. 618–623, 2017, doi: 10.1109/PERCOMW.2017.7917634.

[15] E. Androulaki *et al.*, "Hyperledger fabric," 2018, doi: 10.1145/3190508.3190538.

[16] O. Attia, I. Khoufi, A. Laouiti, and C. Adjih, "An IoT-Blockchain architecture based on hyperledger framework for healthcare monitoring application," *2019 10th IFIP Int. Conf. New Technol. Mobil. Secur. NTMS 2019 - Proc. Work.*, 2019, doi: 10.1109/NTMS.2019.8763849.

[17] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for IoT," *Sensors (Switzerland)*, vol. 19, no. 2, pp. 1–17, 2019, doi: 10.3390/s19020326.

[18] A. D. Dwivedi, L. Malina, P. Dzurenda, and G. Srivastava, "Optimized blockchain model for internet of things based healthcare applications," *arXiv*. IEEE, pp. 135–139, 2019.

[19] S. Biswas, K. Sharif, F. Li, B. Nour, and Y. Wang, "A scalable blockchain framework for secure transactions in IoT," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4650–4659, 2019, doi: 10.1109/JIOT.2018.2874095.

[20] M. A. Rashid and H. H. Pajooh, "A security framework for iot authentication and authorization based on blockchain technology," *Proc. - 2019 18th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. IEEE Int. Conf. Big Data Sci. Eng. Trust. 2019*, pp. 264–271, 2019, doi: 10.1109/TrustCom/BigDataSE.2019.00043.

[21] "Peers — hyperledger-fabricdocs master documentation." https://hyperledger-fabric.readthedocs.io/en/release-2.2/peers/peers.html?highlight=validation#phase-3-validation-and-commit (accessed Apr. 22, 2021).