# Exploration of Medical IoT security with blockchain

Abdou-Essamad Jabri, Mostafa Azizi, C. Drocourt, Gil Utard

# Exploration of Medical IoT security with blockchain

Abdou-Essamad Jabri [1, [0009-0003-3510-0087]], Mostafa AZIZI [1,[0000-0001-9936-3001]], Cyril DROCOURT [2, [0000-0003-1636-9462]], and Gil UTARD [2, 0000-0003-3081-6185]

[1] MATSI, ESTO, UMP, Oujda, Morocco
[2] MIS, UPJV, Amiens, France
{abdou-essamad.jabri, azizi.mos}@ump.ac.ma
cyril.drocourt@u-picardie.fr
gil.utard@u-picardie.fr

**Abstract.** With the widespread adoption of IoT devices and solutions, their security at various levels has become an important concern of professionals and researchers. This issue takes more risk, especially with the IoT variants, IIoT (Industrial IoT) and MIoT (Medical IoT). Many existing security solutions are adapted and proposed for addressing IoT security. In this paper, we are interested in exploring blockchain technology and studying its applicability for MIoT devices. Blockchain technology provides a decentralized, autonomous, trustless, and distributed environment; it is a robust candidate for reinforcing the existing security. Whereas it should be deployed smartly to avoid its practical drawbacks related to energy-consuming and excessive computing. This is well done with a hybrid infrastructure combining IT and IoT networks. As proof of work, we start as a first phase of an ongoing project to implement our blockchain on a distributed virtual environment, including 5 virtual machines running RaspberryPI OS. RaspberryPI OS, distributed by Raspberry Pi Foundation, is based on the Debian Linux distribution, and well optimized for the use on the compact single-boards Raspberry Pi with ARM CPUs. As a blockchain platform, we opt for the use of the open source private blockchain framework, Hyperledger Fabric (HF). As feedback from this investigation, including literature review of recent works and our implementation, we confirm the meaningful contribution of blockchain for enhancing the security of MIoT devices, but this should be reinforced by other security solutions to fulfill the requirements of Zero Trust Architecture.

**Keywords:** IoT, Blockchain, RaspberryPi, Authentication, Data Privacy.

## 1 Introduction

The Internet of Things (IoT) is one of the potential technologies of Industry 4.0, and in particular its industrial variant IIoT. IoT is getting widely used in our everyday lives. With IoT services, we can build smart hardware and software solutions ranging from complex to simple systems, in combination with other technologies such as Networking, Big Data, AI, etc. Surely, at the beginning, manufacturers and users were most steered by fastly creating IoT-based solutions and products and so reducing the time-to-market, and the security issue was not considered a priority, and now it has become critical. Its applications are being threatened by various malicious attacks, and seeked by criminal hacking activities. With the widespread use of IoT and security

omission, IoT systems are running a significant risk and can compromise other IT infrastructures. Let us imagine the negative impact and damage of successful attacks over IoT systems involved in healthcare, finance, smart cities, smart factories, smart homes, …

As most IoT systems are parts of an existing networking architecture, or at least are in interaction with it, to convey the data/commands flows to/from remote servers, clients, or other IoT devices, they are impacted by the same network attacks, to which we add specific IoT attacks, related sensor services and IoT protocols. Nowadays, many researchers and organizations work on the adaptation of existing security solutions to the case of IoT networks and systems, seeking to enhance their security. In the literature, we find many examples of these IoT adapted solutions, such as lightweight IDS, Access control, device authentication, data encryption, blockchain, etc. Some of them fit better the IoT security needs, but are not enough, they should be reinforced by others; Certains techniques are more energy-consuming and should not be deployed directly on sensors or devices with limited resources. Here, in this paper, we are interested in exploring again blockchain technology and studying its applicability for medical IoT (MIoT) devices. As known, blockchain tech delivers a decentralized, autonomous, trustless, and distributed environment; it is a priori a suitable candidate for reinforcing the existing security. On the other hand, the MIoT devices have become widely used in medical campuses (hospitals, clinics, and homes of patients); and their security, locally or with the IT infrastructure of the medical facility, is a critical issue for the privacy and the protection of patients' data (live or archived data). This topic is attracting both professionals and researchers as a hot research trend.

The rest of this paper is structured as follows: Section 2 provides a background on the IoT and Blockchain. Next, in Section 3, we delve into the literature review of related works. While Section 4 deals with a case study on the implementation of the Hyperledger fabric framework on virtual machines running Raspberry PI OS. Afterwards, we conclude this work by stating some recommendations and standing some perspectives.

## 2 Backgrounds

### 2.1 IOT

The coming of IoT [1-21] was in the vision to widen the known Internet and to make it more inclusive and open to bring everything under its umbrella, objects ranging from common devices to animals and humans, with the ability to directly transfer or receive data over a network. In short, an IoT system consists of various cyber-physical devices such as sensors and actuators, with an infrastructure of connectivity to fog or cloud levels. When the sensors' data reach its destination on the fog/cloud servers, it will be processed and eventually some decisions will be taken and transmitted as actions to perform by actuators. For interaction with humans, a GUI is needed; for example, it is often required to observe the dash-board of the IoT solution and to have an insight of different indicators, and the user can act accordingly and adjust some behaviors.

By massively using sensors for generating live and real-time data, we are creating analytically rich and representative datasets that professionals need for solving, with machine learning or other statistical modeling techniques, complex problems in healthcare, finance, logistics, manufacturing … IoT and its variants IIoT and MIoT are key tools for increasing efficiency and control of different systems from various domains. For example, MIoT helps to improve the health and in-crease the safety of patients, in their homes or even in hospitals, by enabling remote surveillance and monitoring of their medical states (see Figure 1).

Unfortunately, each IoT device, connected to the internet, quickly becomes a target for hacking. By hubbing sensors and actuators on gateways, we can reduce the number of devices connected to the internet; they are only connected to gateways and are hidden behind them. This is why the gateways are more threatened and their security should be strengthened.

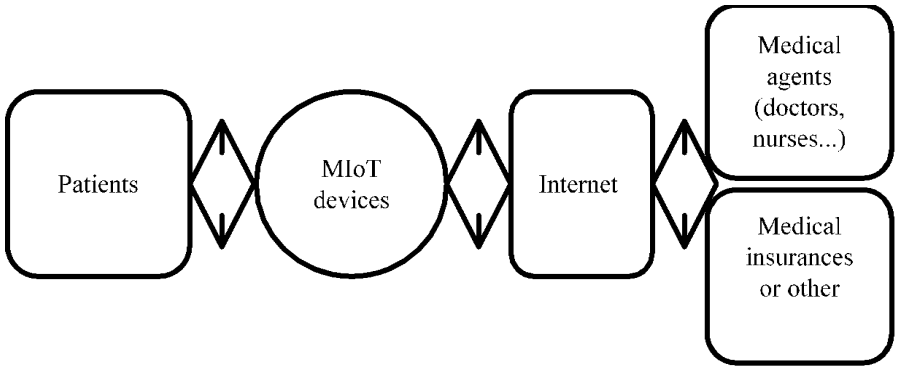


**Fig. 1.** A simplified medical data chain with MIoT devices

## 2.2 **Blockchain**

A blockchain [1-21] is a distributed and decentralized ledger shared among joined network nodes so that to maintain it secure and immutable, as a decentralized record of data transactions (see Figure 2). This ledger stores data in blocks linked together via cryptography. Each block is hashed, and its hash is used as a link into the next block header. This creates a series of encrypted blocks that are chained together.

A blockchain uses scripts that manage the ledger and keep up-dated and validated its distributed copies on many nodes. To automate transactions, the concept of smart contracts is considered; a smart contract is a code with a set of agreed conditions, once the conditions are fulfilled, the corresponding agreement is automatically carried out.

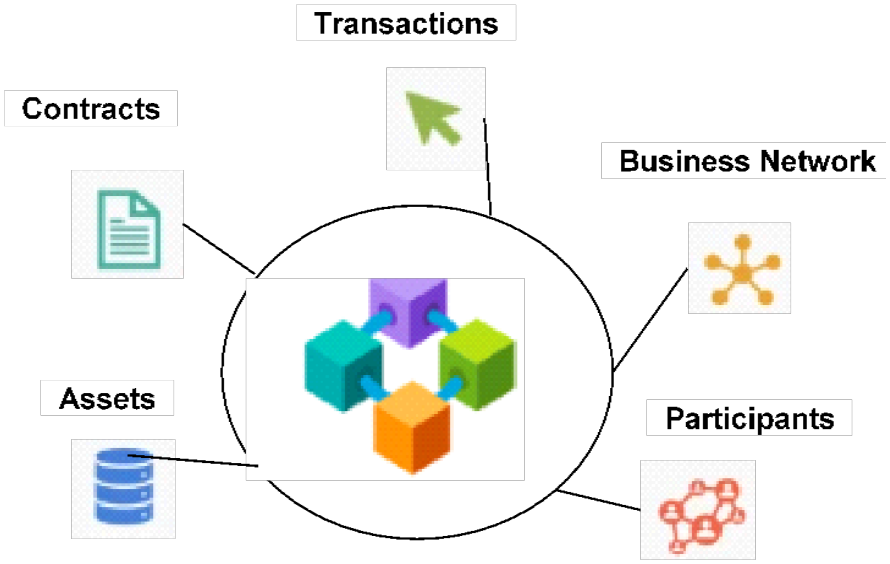


**Fig. 2.** General Blockchain View

We distinguish three types of blockchain: private blockchain, public blockchain, and hybrid blockchain. A public blockchain is a permissionless and open blockchain, anyone can join the network freely and establish a node under conditions of use. A private blockchain is a permissioned blockchain, each node should be approved before joining. On the other hand, a hybrid blockchain mixes public and private blockchains.

Currently, numerous projects are looking to implement blockchains in several ways to help companies and organizations secure their data recording transactions (see Figure 2). These data records could be anything valuable, like votes in elections, money transfers, healthcare records … It depends on the business logic of the partners. Blockchain is in its third decade, and its applications are countless; Now-a-days, we count 23000 active cryptocurrencies and hundreds of thou-sands of applications from various sectors. For instance, in healthcare domains, providers can implement a blockchain for securely storing and exchanging their patients' medical records. Acting this way ensures that a medical record cannot be illicitly changed, and it is encrypted and only accessible to authorized individuals.

## 3 Related works

### 3.1 Selection of papers

This section describes our methodology for reviewing recent papers on IoT and Blockchain in the medical context. Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) guidance were followed. The search for articles was conducted in Web of Science and ScienceDirect. Therefore, to select the papers considered for this review, we have applied this search criteria "IoT AND Security

AND Blockchain," "Medical IoT AND Blockchain," and "IoT AND healthcare AND Blockchain" over the last five years. At the end, we got through this filter 22 papers. Furthermore, we add three of our works to end up with 25 papers. All these works [1-24] will be examined in the following subsection.

### 3.2 Review of the selected papers

[1] gives an overview of IoT security problems, it steps on the three layers considered for IoT (perception layer, network layer and application layer), and dis-cusses the specific issues for each level. It promotes using a high-level security management scheme based on blockchain for different IoT devices in the full life cycle. While [2] presents a survey in the same way, it again skims through security and privacy challenges of the adhoc IoT systems, ranging from the infrastructure devices, through protocols, to applications. It also covers IoT security solutions based on various technologies, like Machine learning, Artificial intelligence, and Blockchain, to target CIA objectives.

In [3], the authors propose the SCNCQB-TSTP protocol (Service Constraint Network Condition and Behavior Quality-Trust orient secure transmission proto-col) that aims, on one hand, to secure transmission by analyzing various factors of network, user behavior and quality of service, and selecting the more trusted route (with best secure transmission score) among others to reach the service point; then, on the other hand, it uses blockchain technology for ensuring data security. The transmission could involve devices from edge, fog, or cloud computing levels. [4] proposes an intelligent and fuzzy blockchain-based framework that involves a fuzzy DL model towards attack detection. It allows to identify and detect security threats in case of uncertainty issues in IoT networks and having more flexibility in decision-making and accepting transactions in the blockchain layer. The combination of DL with fuzzy logic reinforces the capacities of blockchain when all deployed within IoT networks. [5] makes a review of the available blockchain solutions to examine their compliance with IoT systems like those of smart homes. It concludes that the majority of blockchain platforms do not meet the target requirements in terms of privacy, consensus protocols, and fault tolerance. [6] discusses the growing interest in Blockchain due to its unique qualities like auditability, security, and anonymity. It mentions its applications beyond finance, such as in IoT, but highlights that Blockchain's computational expenses and scalability issues make it less suitable for IoT. [6] introduces a solution called Lightweight Scalable Blockchain (LSB) tailored for IoT, utilizing an overlay net-work and a Distributed Time-based Consensus algorithm for efficiency. This approach is tested in a smart home scenario and shows improved scalability and reduced delays compared to similar systems. [7] surveys the use of IoT in various domains, along with its vulnerability to hacking due to limited resources in IoT devices. It highlights major security concerns in IoT, categorizing issues across architecture and protocols. The role of blockchain in addressing IoT security prob-lems is explored, drawing parallels to its use in Bitcoin. [8] introduces the concept of blockchain as a trustworthy distributed system and proposes a lightweight IoT security framework based on blockchain. This framework combines data and transaction blockchain flows, enhancing data storage and transaction efficiency. It employs algorithms like PBFT for consensus and partial blind signatures for privacy. The framework addresses malicious behavior through node

cooperation dynamics and reputation estimation, achieving a secure and effective system for IoT devices with verified location information. Simulation experiments demonstrate its anti-attack capability and processing efficiency. [9] highlights the widespread interest in blockchain technology, extending beyond its origins in cryptocurrencies to various domains like finance, logistics, IoT, and cybersecurity. It discusses the evolution of blockchain and emphasizes the convergence of block-chain and the Internet of Things (IoT), citing existing deployments and initiatives. This paper also outlines the mapping between blockchain and IoT and its significance in various sectors. [10] discusses the challenges faced by the Internet of Things (IoT) due to limited computing capacity and security issues. It proposes a solution that integrates a security gateway architecture for IoT devices with Blockchain technology to enhance decentralization, authentication, and anonymity. This approach improves data reliability through compatible cryptographic algorithms and ensures compatibility with all IoT products, making it suitable for tasks like microgrid trading over advanced network infrastructures. The solution includes a security procedure supporting various cryptographic algorithms and is safeguarded by Blockchain to establish trust and eliminate single control authority. [11] discusses the growing significance of Blockchain in criminal investigation due to increasing security threats across various industries like Electronic Health Record (EHR), banking, smart applications, supply chain management, and IoT. A novel framework is introduced, utilizing a Cloud-based Software Defined Network (SDN) with 100 mobile nodes (as IoT devices), open flow switches, Blockchain controllers, and servers (authentication …). The system employs ECIES encryption and signature methods, allowing authorized investigators to perform identification, evidence collection, analysis, and report generation using a Logical Graph of Evidence (LGoE). The proposed system demonstrates improved performance in terms of response time, accuracy, throughput, and security. [12] highlights how blockchain technology enhances security in various applications, including healthcare and IoT. It discusses the benefits of using blockchain in the healthcare sector, improving security, privacy, transparency, and efficiency. The proposed application (PA) utilizes blockchain to generate, maintain, and validate healthcare certificates, acting as a secure communication medium between hospitals, patients, doctors, and IoT devices. The system incorporates features like confidentiality, authentication, and access control through smart contracts, outperforming existing solutions in terms of effectiveness. [13] addresses the security challenges in smart cities' IoT networks due to the growth of insecure devices. Existing security mechanisms face issues like inefficiency and data collection. The paper proposes a decentralized security architecture combining Software Defined Networking (SDN), blockchain, and Fog/Mobile Edge Computing. SDN continuously monitors network traffic, blockchain offers decentralized attack detection, and Fog/Edge Computing enables efficient early detection and mitigation. Experimental evaluation demonstrates that the proposed architecture outperforms centralized and distributed approaches in terms of accuracy and detection time. [14] discusses the rapid growth of healthcare with IoT and wearable devices, emphasizing the security challenges in client/server architectures for remote patient monitoring. It proposes "BlockMedCare," a secure healthcare system integrating IoT with Blockchain to address these challenges. The system employs re-encryption, Blockchain storage, smart contracts for access control, and IPFS for scalability. Ethereum-based proof of authority is used to speed up data storage, focusing

on security, scalability, and processing time. The proposed system is applied to diabetes management, demonstrating improved healthcare security compared to existing methods.[15] discusses the rise of the Internet of Things (IoT) and its extension into the Industrial Internet of Things (IIoT), highlighting the increased security challenges in both domains. The survey classifies attacks based on vulnerabilities and maps them to IoT/IIoT architecture layers, presenting countermeasures from literature and real-life attack examples. It explores security threats in IIoT, including case studies, and delves into how blockchain, particularly Tangle, can address challenges posed by centralized architectures. The text also outlines Blockchain-based solutions and identifies open research directions for IoT/IIoT security. [16] discusses the role of the Internet of Things (IoT) in achieving a common operating picture (COP) across different applications. It mentions that while IoT has benefits, it also raises security and privacy concerns due to central server reliance. To address this, blockchain technology is introduced to IoT to enhance security. The paper explores security and privacy issues, focusing on how distributed ledger-based blockchain contributes to IoT, and it delves into applications and challenges related to this integration. [17] discusses the expanded attack surface resulting from Internet of Things (IoT) deployment and the need for end-to-end security. It highlights the diverse range of IoT applications, both mission-critical and business-oriented, and the requirement for comprehensive security. Blockchain mechanisms (BCMs) are introduced as part of a security strategy to secure various IoT applications, creating a tamperproof database for transactions. The paper emphasizes the role of BCMs in specific IoT environments while noting that they are just one component of a broader IoT security solution. [18] discusses the challenge of analyzing and processing massive data in the Power IoT (PIoT) due to limited device capacities, leading to encrypted cloud storage. Key security becomes crucial for data privacy in PIoT, and the proposed solution, Blockchain-Assisted Threshold Cryptography for Key Security Management (BCTC-KSM), uses a threshold secret sharing algorithm to split symmetric keys and record their rotation history on a blockchain. Attribute access control policies are used to restrict user access to key fragments. The solution enhances security and availability in PIoT data sharing, with a slightly higher time cost compared to existing cryptography schemes. [19] discusses the Internet of Things (IoT) as a future infrastructure with interconnected devices across various industries, including education. It highlights the use of Quick Response (QR) codes for daily transactions, particularly in the context of student attendance tracking. The study aims to create a reliable and secure data interchange system for IoT in education, utilizing 64-bit processor architectures like arm64 and amd64 to develop an attendance system with blockchain technology. The study successfully builds and integrates various components, including Hyperledger Fabric blockchain, QR codes, and Raspberry Pi, to enhance the security and efficiency of the attendance system. [20] discusses Blockchain's potential to address IoT limitations like data protection and privacy but notes its challenges including complexity and scalability. It presents an Efficient Lightweight integrated Blockchain (ELIB) model designed for IoT needs, with a focus on a smart home scenario. The ELIB model employs shared keys and overlay networks for resource-constrained devices, optimizing with lightweight consensus, certificateless cryptography, and Throughput Management. Simulation results show ELIB outperforms baseline methods, with 50% processing time savings and minimal energy consumption, demonstrating its effectiveness in various evaluation parameters. [21]

highlights IoT's emergence and its role in various domains, emphasizing issues like interoperability, data volume, energy efficiency, and security. It introduces a study that integrates blockchain with software-defined networking (SDN) to address these challenges. The proposed approach employs a blockchain-based architecture with a cluster structure routing protocol, enhancing energy efficiency and security. Through experimental results, the study shows improved energy consumption, network throughput, and packet latency compared to existing protocols, particularly benefiting industrial cyber physical systems. [22] proposes a stratified and hierarchized DL-based IDS (SDL-IDS) for the IoT environment at its three levels: Edge, Fog, and Cloud, to enhance the security of IoT networks. SDL-IDS is composed of three blocks that act in collaboration: EdgeIDS, FogIDS, and CloudSIEM. Not all the solutions at the edge level fit the edge devices with limited resources, an adaptation is required. This is what [23] deals with and makes an analysis of the possibility to deploy a Deep Learning-Based Host-Intrusion Detection System (DL-HIDS) on some specific commercial IoT devices. It considers some criteria, such as memory consumption and inference timing, and checks whether the proposed lightweight DL-HIDS fits better to the given device under the announced criteria. As obvious, hackers are continuously developing new attacks to defeat the existing IDSs, and consequently these IDSs should be also updated and strengthened. In this regard, [24] presents a solution for updating DL-IDS employing a transfer learning technique that allows us to retrain and fine-tune pre-trained models on small datasets with new attack behaviors. On the other hand, [28] proposes an authentication delegation protocol based on the use of PREs that can be used in the IoT context; Connected objects require to work on personal data and therefore need to be authenticated, without having access to a permanent Internet connection. In this regard, [29] presents an authentication and authorization architecture for IoT-based healthcare using smart gateways for more security and efficiency.

### 3.3 Recapitulation

Next the review of all these papers, we make the following constatations:

- IoT and its variants have been widely deployed in different domains and applications, from complex to simple, and from critical to ‘don’t care.’ Along with this, users are overly concerned about the security of the critical IoT devices, such as MIoT ones.
- To implement this required security, many authors propose using blockchain technology, especially for ensuring safe data communication.
- However, blockchain alone is not enough, and it should be reinforced by other complementary security techniques.

## 4 Case study: exploration and implementation of blockchain over a cluster of Raspberry PI machines

To confirm our review’s conclusions, we launch an ongoing project with two stages. The first stage consists of deploying the aforementioned concepts in a virtual environment, while the second stage, as a future work, will focus on conducting the experimentation on a real environment (with Raspberry PI boards [25, 27, 29]). We

consider a network with 5 nodes (see Figure 4); each node is a virtual machine Pi (i=1...5) running Raspberry PI OS and is fully connected to the other nodes. Then, we make the installation and settings of the blockchain, Hyperledger Fabric. Within this virtual context, the sensors' data streaming is simulated using random functions; We here focus on the evolution of the body temperature, the blood oxygen, the blood pressures, and the heart beats.

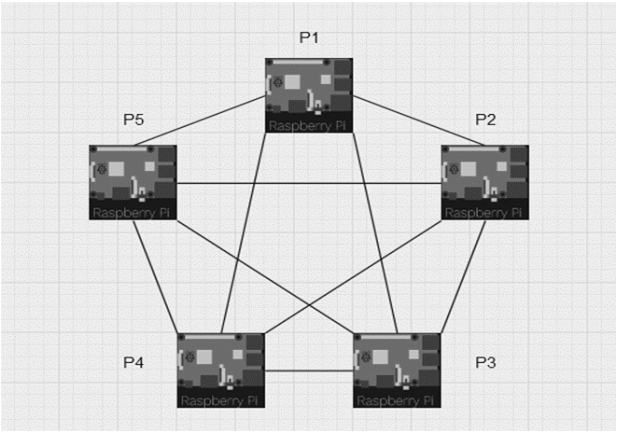


**Fig. 3.** Communication diagram of our miniature MIoT network with embedded blockchain

In opposition to an open and permissionless system, Hyperledger Fabric [26] is a scalable and secure platform that supports private transactions and confidential contracts. A such framework allows to develop solutions adapted for any industry, with trust, transparency, and accountability for businesses. We recall that the ledger consists of a blockchain B linking the different blocks (B1, B2 …), and a World state database keeping update the values of the different transactions (T1, T2 …) (see Figure 5). Each transaction within any block is signed and verified; Every block is hashed and added at the queue of the blockchain (see Figure 6). These transactions are watched by smart contracts before granting or refusing their execution. Doing so, we can automate the execution of transactions once the requirements expressed in the contract have been fulfilled. Most of the contracts in our case are involved in the ownership authentication and the data access control regarding different actors (machines, patients, doctors, medical staff, insurance …).

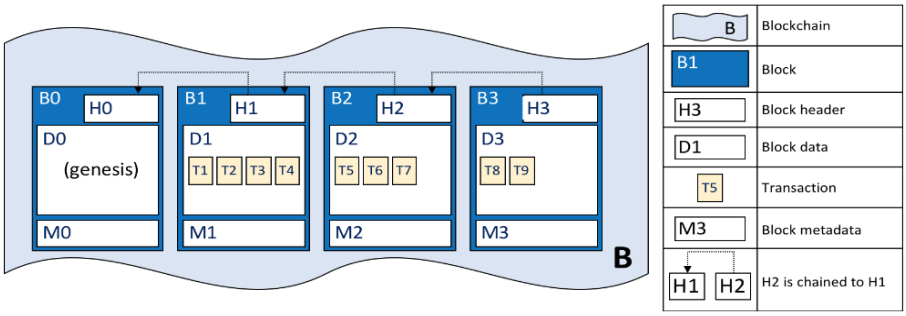


**Fig. 4.** Blocks of Hyperledger Fabric

```
class Transaction:
    ...
class Block:
    ...
    def calculate_hash(self):
    ...
    def mine_block(self, difficulty):
    ...
class Blockchain:
    ...
    def create_genesis_block(self):
    ...
    def add_block(self, new_block):
    ...
    def is_chain_valid(self):
    ...
def generate_key_pair():
    ...
def sign_transaction(private_key, transaction):
    ...
def verify_transaction(public_key, transaction, signature):
    ...
```

**Fig. 5.** Blockchain implementation

In this first stage of our ongoing project, we have explored blockchain technology and illustrated its different components. In addition, we are now aware of the complexity to put it in use, and well prepared to go further involving sensors through the Raspberry PI boards in the next stage. Securing MIOT devices using blockchain technology offers several advantages that address the limitations of existing security methods. Thanks to its decentralized architecture, Hyperledger Fabric eliminates single points of failure and unauthorized access, while the immutability of the block-chain ensures data integrity and prevent tampering. The transparency and auditability of

blockchain transactions allow a comprehensive tracking of devices' activities and identification of anomalies. Blockchain based authentication and authorization mechanisms provide secure and flexible access control, while secure channels and controlled data access address privacy concerns and enable secure data sharing among authorized entities.

## 5 Conclusion

In this paper, we have explored blockchain technology and studied its applicability for MIoT devices. Blockchain technology provides a decentralized, autonomous, thrustless, and distributed environment; it is a robust candidate for reinforcing the existing security. Whereas it should be deployed smartly to avoid its practical drawbacks related to energy-consuming and excessive computing. As feedback from the reviewed papers, blockchain is a potential security solution for IoT and its variants, including MIoT. In this regard, we have launched the first phase of our ongoing project, by implementing a blockchain on a distributed virtual environment, including 5 virtual machines running RaspberryPI OS. We opt-ed for using the open source private blockchain framework, Hyperledger Fabric (HF). Following this investigation, including literature review of recent works and our implementation, we confirm the meaningful contribution of blockchain for enhancing the security of MIoT devices, but it is not enough; Other security solutions should be deployed to fit the requirements of recent security policies, such as Zero Trust Architecture.

**Acknowledgment:** This work is partly supported by the Hassan II Academy of Sciences and Technologies and Mohammed First University.

## 6 References

1. Yongfeng Qian, Yingying Jiang, Jing Chen, Yu Zhang, Jeungeun Song, Ming Zhou, Matevž Pustišek (2018), Towards decentralized IoT security enhancement: A blockchain approach, Computers and Electrical Engineering 72 (2018) 266–273
2. Bhabendu Kumar Mohanta, Debasish Jena, Utkalika Satapathy, Srikanta Patnaik (2020), Survey on IoT security: Challenges and solution using machine learning, artificial intelligence and blockchain technology, Internet of Things 11 (2020) 100227
3. Premkumar R., S. Sathya Priya (2022), Service Constraint NCBQ trust orient secure transmission with IoT devices for improved data security in cloud using blockchain, Measurement: Sensors 24 (2022) 100486
4. Abbas Yazdinejad, Ali Dehghantanha, Reza M. Parizi, Gautam Srivastava, Hadis Karim-ipour (2023), Secure Intelligent Fuzzy Blockchain Framework: Effective Threat Detection in IoT Networks, Computers in Industry 144 (2023) 103801
5. Sotirios Brotsis, Konstantinos Limniotis, Gueltoum Bendiab, Nicholas Kolokotronis, Stavros Shiaeles (2021), On the suitability of blockchain platforms for IoT applications: Architectures, security, privacy, and performance, Computer Networks 191 (2021) 108005
6. Ali Dorri, Salil S. Kanhere, Raja Jurdak, Praveen Gauravaram (2019), LSB: A Light-weight Scalable Blockchain for IoT security and anonymity, Journal of Parallel and Dis-tributed Computing 134 (2019) 180–197
7. Minhaj Ahmad Khan, Khaled Salah (2018), IoT security: Review, blockchain solutions, and open challenges, Future Generation Computer Systems 82 (2018) 395–411

8. Haiping Si, Changxia Sun, Yanling Li, Hongbo Qiao (2019), IoT information sharing security mechanism based on blockchain technology, Lei Shi, Future Generation Computer Systems 101 (2019) 1028–1040
9. Younes ABBASSIa, Habib Benlahmer (2021), IoT and Blockchain combined: for de-centralized security, Procedia Computer Science 191 (2021) 337–342, The 2nd International Workshop on Artificial Intelligence & Internet of Things (A2IOT), August 9-12, 2021, Leuven, Belgium
10. Marko Šarac, Nikola Pavlović, Nebojsa Bacanin, Fadi Al-Turjman, Saša Adamović (2021), Increasing privacy and security by integrating a Blockchain Secure Interface into an IoT Device Security Gateway Architecture, Energy Reports 7 (2021) 8075–8082
11. P. Velmurugadass, S. Dhanasekaran, S. Shasi Anand ⇑, V. Vasudevan (2021), Enhancing Blockchain security in cloud computing with IoT environment using ECIES and cryptography hash algorithm, Materials Today: Proceedings 37 (2021) 2653–2659
12. Pratima Sharma, Suyel Namasudra, Ruben Gonzalez Crespo, Javier Parra-Fuente, Munesh Chandra Trivedi (2023), EHDHE: Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain, Information Sciences 629 (2023) 703–718
13. Shailendra Rathore, Byung Wook Kwon, Jong Hyuk Park (2019), BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network, Journal of Network and Computer Applications 143 (2019) 167–177
14. Kebira Azbeg, Ouail Ouchetto, Said Jai Andaloussi (2022), BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security, Egyptian Informatics Journal 23 (2022) 329–343
15. Jayasree Sengupta, Sushmita Ruj, Sipra Das Bit (2020), A Comprehensive Survey on Attacks, Security Issues and Blockchain Solutions for IoT and IIoT, Journal of Network and Computer Applications 149 (2020) 102481
16. Nallapaneni Manoj Kumara,Pradeep Kumar Mallick (2018), Blockchain technology for security issues and challenges in IoT, Procedia Computer Science 132 (2018) 1815–1823, International Conference on Computational Intelligence and Data Science (ICCIDS 2018)
17. Daniel Minoli, Benedict Occhiogrosso (2018), Blockchain mechanisms for IoT security, Internet of Things 1–2 (2018) 1–13
18. Song Deng, Qicong Hu, Di Wu, Yi He (2023), BCTC-KSM: A blockchain-assisted threshold cryptography for key security management in power IoT data sharing, Computers and Electrical Engineering 108 (2023) 108666
19. Upahm Abas, S., Duran, F., Tekerek, A. (2023), A Raspberry Pi based Blockchain Application on IoT Security, Expert Systems with Applications, doi: https://doi.org/10.1016/j.eswa.2023.120486
20. Sachi Nandan Mohanty, K.C. Ramya, S. Sheeba Rani, Deepak Gupta, K. Shankar, S.K. Lakshmanaprabu, Ashish Khanna (2020), An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy, Future Generation Computer Systems 102 (2020) 1027–1037
21. Sohaib A. Latif, Fang B. Xian Wen, Celestine Iwendi, Li-li F. Wang, Syed Muhammad Mohsin, Zhaoyang Han, Shahab S. Band (2022), AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems, Computer Communications 181 (2022) 274–283
22. Idriss Idrissi, Mostafa Azizi, and Omar Moussaoui (2022), A Stratified IoT Deep Learning based Intrusion Detection System, In the proceedings of the 2nd International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET), Meknes, Morocco, 2022, pp. 1-8, IEEE Xplore, doi: 10.1109/IRASET52964.2022.9738045.
23. Idriss Idrissi, Mostafa Azizi, and Omar Moussaoui (2021), Accelerating the update of a DL-based IDS for IoT using deep transfer learning, Indonesian Journal of Electrical Engineering and Computer Science Vol. 23, No. 2, August 2021, pp. 1059~1067

24. Idriss Idrissi, Mostafa Azizi, and Omar Moussaoui (2021), A Lightweight Optimized Deep Learning-based Host-Intrusion Detection System Deployed on the Edge for IoT, International Journal of Computing and Digital Systems Vol. 5, No. 3 (May-2021), pp. 189-196
25. https://www.raspberrypi.com (2023)
26. https://www.hyperledger.org (2023)
27. K. Jaiswal, S. Sobhanayak, B.K. Mohanta, D. Jena (2017), IoT-cloud based framework for patient's data collection in smart healthcare systems using raspberry-pi, in: 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA), IEEE, 2017, pp. 1–4.
28. A. Sbai, C. Drocourt, G. Dequen - « A New Delegated Authentication Protocol based on PRE » - SECRYPT 2021, The 18th International Conference on Security and Cryptography, Online Streaming, p. 468-478, 6-8 July 2021
29. S.R. Moosavi, T.N. Gia, A.-M. Rahmani, E. Nigussie, S. Virtanen, J. Isoaho, H. Tenhunen (2015), Sea: a secure and efficient authentication and authorization architecture for IoT-based healthcare using smart gateways, Procedia Comput. Sci. 52 (2015) 452–459.