Retraction Notice

Title of retracted article: **Enhancing Security of IoT by Using Blockchain**

Author(s): Bodoor Al-Rayani

*Corresponding author's Email: balrayani@stu.kau.edu.sa

Journal: Open Access Library Journal (OALib Journal)
Year: 2022
Volume: 9
Number: 8
Pages (from - to): 1-14
DOI (to PDF): https://doi.org/10.4236/oalib.1109148
Paper ID at SCIRP: 119417
Article page: https://www.scirp.org/journal/paperinformation.aspx?paperid=119417

Retraction date: 2024-01-25

Retraction initiative (multiple responses allowed; mark with **X**):
X All authors
☐ Some of the authors:
☐ Editor with hints from
- ○ Journal owner (publisher)
- ○ Institution:
- ○ Reader:
- ○ Other:

Date initiative is launched: 2024-01-17

Retraction type (multiple responses allowed):
☐ Unreliable findings
- ○ Lab error
- ○ Inconsistent data
- ○ Analytical error
- ○ Biased interpretation
- ○ Other:

☐ Irreproducible results
☐ Failure to disclose a major competing interest likely to influence interpretations or recommendations
☐ Unethical research

☐ Fraud
- ○ Data fabrication
- ○ Fake publication
- ○ Other:

☐ Plagiarism
- ☐ Self plagiarism
- ☐ Overlap
- ☐ Redundant publication *

☐ Copyright infringement
- ☐ Other legal concern:

☐ Editorial reasons
- ○ Handling error
- ○ Unreliable review(s)
- ○ Decision error
- ○ Other:

X Other: Authors requested withdrawal.

Author's conduct (only one response allowed):
☐ honest error
☐ academic misconduct
X none (not applicable in this case – e.g. in case of editorial reasons)

* Also called duplicate or repetitive publication. Definition: "Publishing or attempting to publish substantially the same work more than once."

Comment:
The Editorial Board would like to extend its sincere apologies for any inconvenience this retraction may have caused.

Open Access Library Journal
2022, Volume 9, e9148
ISSN Online: 2333-9721
ISSN Print: 2333-9705

Enhancing Security of IoT by Using Blockchain

Bodoor Al-Rayani, Jawaher Al-Harbi, Morooj Al-Ghamdi

College of Computing and Information Technology, King Abdulaziz University, Jeddah, Saudi Arabia
Email: balrayani@stu.kau.edu.sa, jalharbi0086@stu.kau.edu.sa, malghamdi1736@stu.kau.edu.sa

How to cite this paper: Al-Rayani, B., Al-Harbi, J. and Al-Ghamdi, M. (2022) Enhancing Security of IoT by Using Blockchain. *Open Access Library Journal*, **9**: e9148.
https://doi.org/10.4236/oalib.1109148

Received: July 28, 2022
Accepted: August 22, 2022
Published: August 25, 2022

Abstract

In recent years, the Internet of Things has become urgent in our lives, as it is used in many areas to facilitate business and daily life. But unfortunately, there are concerns due to security and safety issues. Therefore, many researchers have turned their attention to identifying the best solutions for increasing security and raising privacy one of which is the usage of Blockchain in the Internet of Things. This paper presents the benefits of applying Blockchain technology to the Internet of Things, the challenges faced and the most up-to-date components that satisfy the Component-Based Development (CBD) principles to enhance security and privacy.

Subject Areas

Computer Science and Engineering

Keywords

Blockchain, IoT, Security and Storing Manager (SSM), Google Cloud Platform (GCP), Smart Contract, Hyperledger

1. Introduction

The Internet of Things (IoT) connects many things over the network and allows communication and interaction among them, such as smartphones, vehicles, and smart cities [1]. However, the traditional Internet of Things faces challenges in several aspects, including security, privacy, and storage capacity, so Blockchain technology has been adopted as an effective solution to the problems of the traditional Internet of Things where can be to ensure data integrity and sensitive data transmission without central servers, as well as provide a security framework for serving IoT components, and for developing IoT using Blockchain technology in the fastest time and lowest cost by applying a Component-Based Development (CBD) approach, which is to develop software based on integrating independent components that can be reused to build a larger

software system which helps increase productivity and improve quality. By using CBD in the IoT-Blockchain this paper introduces two components: Smart Contract and Security and Storing Manager (SSM), which will be discussed in detail as the mechanism that operates and how it will be built.

This paper will explain general definitions of the IoT and the Blockchain also the Blockchain works. In addition, will introduce an overview of the use of the IoT in the Blockchain and display two types of architectures in the general IoT-Blockchain and the specific IoT-Blockchain for components. Then will present the most important part of this paper which is the available components of an IoT-Blockchain. Besides, the framework and platforms are used in IoT-Blockchain. Finally, the conclusion and acknowledgment will be presented.

2. Internet of Things and Blockchain

This section will introduce an overview of the main terminologies which are the Internet of Things and Blockchain. In addition to the way how the Blockchain works, to give a full understanding of the main concepts in this paper.

2.1. Internet of Things

Internet of Things has become an integral part of our near future as it will be the main influencer on the quality of life. It can be seen in using a smartphone to control air conditioning or a smart vacuum when the packing machine sends messages to inform that stock will almost be done, or when self-driving cars reach their destination by choosing the shortest path, and so on. All these examples will be part of our daily life.

The beginning of the emerging Internet of Things term that commonly known as IoT and to call it that name for the first time by Kevin Ashton in 1999 at the Massachusetts Institute of Technology (MIT) by connecting Radio-Frequency Identification (RFID) to the internet, and since that time it had been developed to be more than using (RFID). It can be defined in simple words as a network of objects/items/things that involve sensors and are connected over the Internet which can be able to transmit, process, exchange, and share the data, affect each other, or be affected remotely to the purpose of keep tracking, monitoring, remembering, reorganizing and control of the processes [1].

The word Things on the Internet of Things could be any physical devise or object embedded with a sensor as previously stated. Also, IoT has been used in a variety of sectors in life such as smart industries, smart cities, and others, the majority of these applications are depicted in **Figure 1**.

2.2. Blockchain

Blockchain technology was applied to Bitcoin Cryptocurrency by Satoshi Nakamoto in 2008 and since that time it had been widely used in different fields such as Smart Contracts, supply chain, healthcare, etc. Blockchain works by linking blocks or entries which are stored data to the next block in sequence order. Its

peer-to-peer network characterizes as a distributed database, decentralizes viz there is no third party, also as a ledger in the sense that blocks cannot be modified or deleted in addition, it's using asymmetric key encryption to secure data. [2].

2.2.1. Blockchain Working

As mentioned before Blockchain consists of ledger blocks of transactions through peer-to-peer networks and every block has a pointer to the preceding block. These transactions are indicated by time-stamped and it's managed by a set of computers using specific algorithms each one of the computers is referred to as a node that shares the same data copy. Also, whoever performs the previous operation is called a miner.

As seen in **Figure 2** each block in Blockchain consists of a Blockchain version to keep an update of protocol, a nonce value which is a number used one at a time by miners in solving a mathematical puzzle to generate a new block. In addition, the hash value of the preceding block includes a cryptographic hash function that helps to protect and secure the chain. In addition to Merkle Root which helps to verify blocks, also Timestamp indicates the time of transactions to take place. Finally, the transaction list which contains all transaction occurs in a particular block [3].

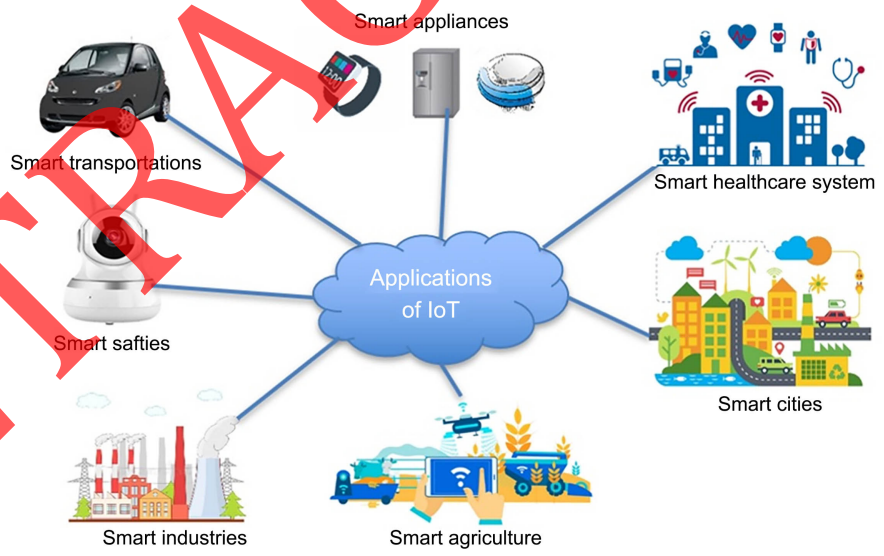

Figure 1. Applications of IoT.

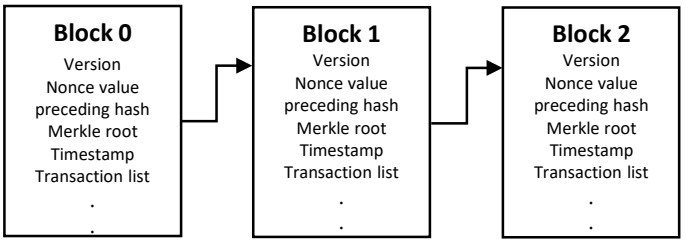

Figure 2. General structure of blocks in blockchain.

2.2.2. Blockchain Versions

Over time, Blockchain has been developed and enhanced to the point that it now has four versions, each of which is summarized by its name, usage, and an example of where to use that version, as shown in Table 1 [4].

3. Overview of Blockchain Usage in IoT

This section discusses the purpose of using Blockchain in the Internet of Things, presents the main advantages, and provides challenges that face the integration of IoT with Blockchain.

3.1. Using Blockchain in IoT

Although the traditional Internet of Things has features including data sharing, real-time analysis, and traceability, these features lack security [5]. It is a prerequisite to be provided in all applications to protect data, and one of the most important issues in the IoT is that it collects data within the central servers. This makes the infrastructure ineffective for processing a large amount of data in IoT systems and this has helped hackers to exploit weaknesses in the infrastructure and expose it to many attacks such as Distributed Denial-of-Service (DDoS), eavesdropping, and other security threats [6], so Blockchain technology has been used to enhance security and overcome these challenges by providing a distributed system or decentralized network [7], as shown in Figure 3.

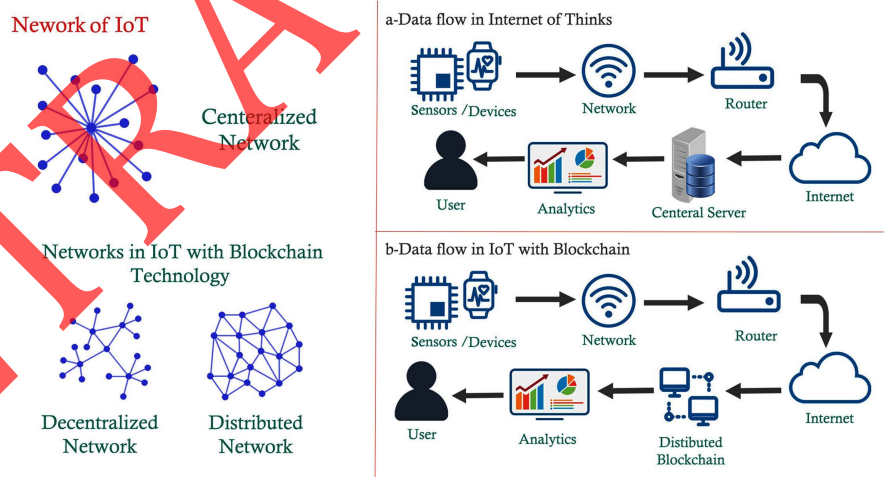

Figure 3. (a) Data flow in IoT, (b) Data flow in IoT with blockchain.

Table 1. Blockchain versions.

Version	Named by	Uses for	Example
Blockchain 1.0	Cryptocurrency	Currency and payments	Bitcoins
Blockchain 2.0	The Smart Contract is a program that executes automatically when the conditions are met.	Swap of money or delivery of services, etc.	Ethereum
Blockchain 3.0	DApps are known as a decentralized application.	Remove single point of failure (SPF) in a centralized application.	Ethereum Swarm
Blockchain 4.0	Industry	Cyber-physical systems	IoT

In Table 2, the characteristics of both technologies are compared, which will show the need for IoT systems to use Blockchain technology to improve their systems in terms of security and architecture. Because Blockchain technology helps IoT systems process huge data, ensure data integrity, increase reliability, and maintain the privacy of digital identity [8]. Sensitive data can also be exchanged and processed without a central server or third-party intervention [9].

3.2. Advantages of IoT-Blockchain

Blockchain technology is considered one of the best solutions capable of supporting the Internet of Things systems in terms of security and a decentralized ecosystem. One of the results of combining the two techniques is the emergence of several advantages as shown in Figure 4 [10] [11].

Decentralization Blockchain technology is characterized by this feature, which makes it able to manage security and achieve trust, unlike the central administration. In the Blockchain, transactions at each node are periodically checked for approval and added to the ledger. This makes them able to control synchronous traffic, eliminating a single point of failure and making IoT systems secure.

Fault tolerance in Blockchain technology, an error can be tolerated as data can be preserved and never lost. Each node contains a copy of all the transactions that occurred in the network, which means that attacking or failing a single node does not cause data loss in IoT, and it also increases the storage problem in the Blockchain and IoT.

Table 2. The characteristics of both technologies IoT and blockchain.

	IoT	Blockchain
Network	Centralized	Completely decentralized or distributed network
Security and privacy	Intermediate security and privacy	Higher security and privacy
Cost maintenance	High cost	Low cost and speed maintenance
Reliability	Data can be manipulated	The data cannot be modified or manipulated
Redundancy	Single point of failure	Multiple points of failure

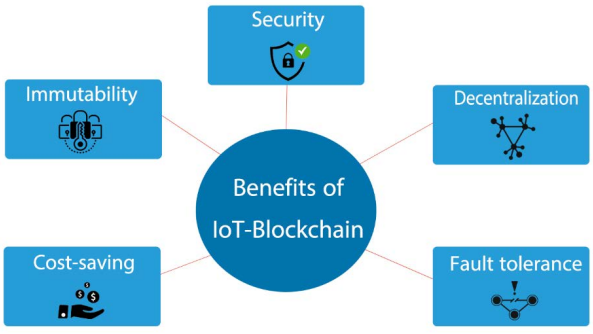

Figure 4. Advantages of IoT-blockchain.

Security provides a secure network through anonymity and privacy preservation as it encrypts digital identity using a hash algorithm and public-key cryptography [12], allowing IoT applications to securely exchange sensitive information over the network.

Cost-saving with the increase in the use of the Internet of Things and the large number of devices connections to the network, it is difficult to deal with it in the case of using central servers, as it increases the cost of maintenance and infrastructure. But with the decentralization of IoT systems by Blockchain technology, this problem was overcome, which improved the maintenance process and upgraded the system faster and at a lower cost.

Immutability the data in the ledger is fixed and not easily modified or deleted, which distinguishes Blockchain technology, which increases the security and integrity of data in the Internet of Things applications.

This shows that IoT applications based on Blockchain technology are more secure than traditional IoT applications.

3.3. Challenges of IoT-Blockchain

Although IoT-Blockchain has unlimited advantages, it faces some challenges as shown in Figure 5. The challenges it faces can be summarized as follows: [10] [11]

Scalability IoT resources are limited in storage and connectivity, unlike Blockchain technology, but the consensus, computation process of algorithms, and storing the record of transactions require more storage capacity in the cloud to avoid centralization.

Processing power and speed the speed of processing and encryption are very important in Blockchain technology, but due to the different types of IoT devices and their different computing capabilities, the encryption process is one of the challenges facing the Blockchain because it is not possible to run the same algorithm on all devices and achieve the same required speed.

Lack of skills the process of integrating IoT technology with the Blockchain is new, so it requires sufficient awareness in dealing with it and understanding the way the Blockchain works in general, especially in banking institutions and other applications.

The error cannot be modified if a transaction is permanently published on the Blockchain, it cannot be reversed. If there is an error in the data stored in the

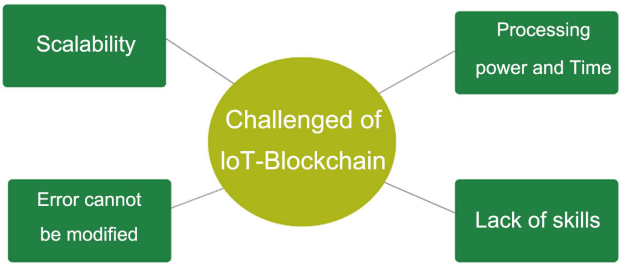

Figure 5. Challenges of IoT-blockchain.

transaction records, it cannot be modified because the transaction records are not automatically transferred to a new record for updating.

4. IoT-Blockchain

This part of the paper considers two types of architecture general IoT-Blockchain architecture and the specific architecture for the component that offers security and privacy of the data.

4.1. General IoT-Blockchain Architecture

There are different types of IoT-Blockchain architectures, but they can be drawn in general as five layers which are shown in Figure 6. This architecture collects the main characteristic of Blockchain and IoT systems. The first layer is the physical layer that is considered as same in IoT and Blockchain that contains the sensors, phones, RFID tags, and all applications of IoT-Blockchain. The second is the network layer that is in charge of internetworking, routing, and multicasting among IoT devices, also both IoT and Blockchain have the same network layer. The third layer is the Blockchain layer that is responsible for applying Blockchain processes in IoT-Blockchain such as sharing and storing data. The fourth layer is the middleware layer where both IoT and Blockchain differ from each other, however, it's accountable for managing Blockchain, achieving integration of services, and supplying security services. The fifth layer and the last one is the application layer that presented interactions, services, and Application

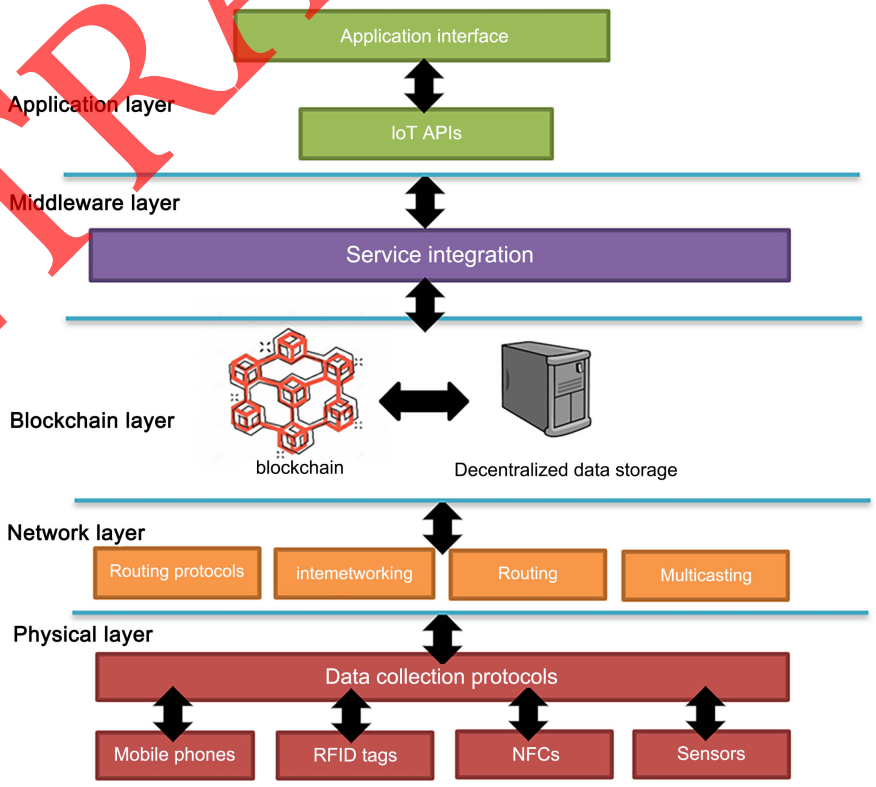

Figure 6. General IoT-blockchain architecture.

Programming Interface (API) functions to users, also both IoT and Blockchain have the same application layer.

As seen before the physical layer, the network layer, the Blockchain layer, and the application layer all were similar in IoT and Blockchain systems, the main difference was in the middleware layer. In this structure can say the IoT was responsible for generating and gathering data while the Blockchain was responsible for securing and saving data [9].

4.2. Specific IoT-Blockchain Architecture

In this architecture, there are three layers as shown in Figure 7 the first one is the device layer which includes IoT networks that contain IoT devices. The second layer is the fog-blockchain layer which contains a Blockchain that is connected to the devices via fog nodes, and here appears the benefit of the Security and Storing Manager SSM with Smart Contract components in securing and protecting data, these components and its work will be discussed further in the following section. Finally, the cloud layer which represents the internet where the final Blockchain will be stored [13].

The following section is the most essential part of this paper, as it demonstrates the significance of Component-Based Development CBD and its usage in IoT-Blockchain systems.

5. IoT-Based Blockchain Components

The most pressing concerns in IoT are security and privacy, as the data generated by IoT devices may contain confidential or private data. As a result, new security protocols are needed to protect all those devices and data.

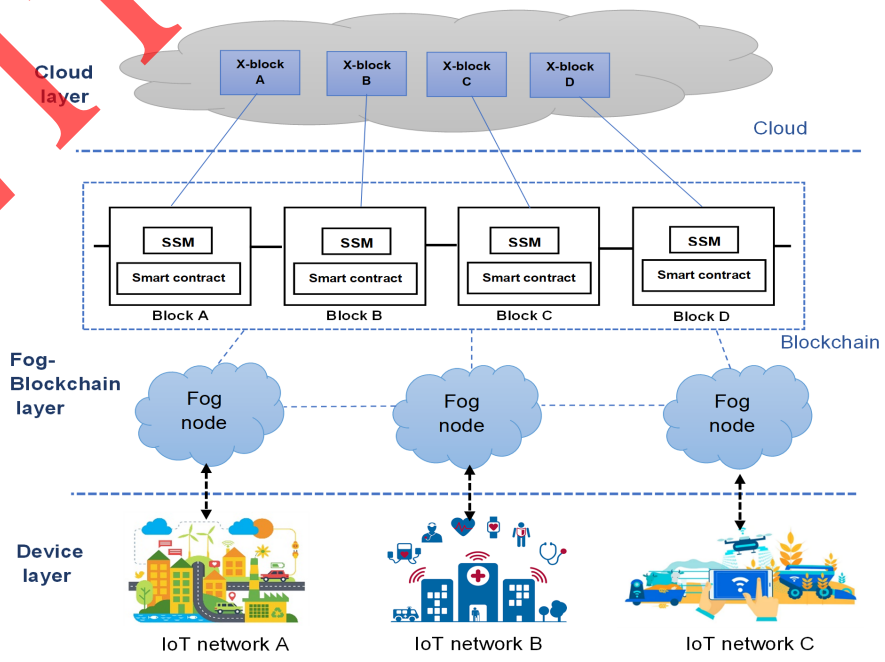

Figure 7. Specific IoT-blockchain architecture.

Blockchain will be used with IoT devices to securely store all data and transactions generated by the devices. However, the Blockchain's design makes it impossible to transport large amounts of data, and transactions on the Blockchain must be public for miners to validate them, resulting in a significant loss of privacy.

For these reasons, the SSM component will be introduced to achieve robust security and privacy goals. Moreover, the attackers may control and compromise millions of IoT devices from anywhere, so the Smart Contract component is important to control and restrict the IoT devices' access.

Both components are reliable, because it audits the huge amount of data being protected, secured, and stored in a distributed manner. Also, these components are considered reusable components which can be used in many IoT-Blockchain applications that save cost and time from to be wasting in a sense it will be used again and again.

5.1. The SSM Component

The Security and Storing Manager (SSM) is a computer program that will run inside the Blockchain. When SSM receives the data, it will automatically execute. The SSM mechanism provides strong security which optimizes both issues of data storage in the Blockchain and privacy and security [13].

5.1.1. The SSM Component Mechanism

The SSM component will create a new locked block (X-Blocks), then will encrypt the main data and store it in the new locked blocks that are generated from each Blockchain using strong encryption algorithms such as Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES)…etc., after that, the encrypted data from each Blockchain will be held on the internet (Cloud), which is the best option since it is limitless, in the new locked block (X-Block). Therefore, the SSM only stores the address of these locked blocks as well as the hash of the data, which is created using a hash algorithm like SHA-256 to create a digital signature of data on the Blockchain. No one knows where the locked blocks are, and even if they were somehow found, impossible for anyone would be able to know what they were [13] as shown in **Figure 8**.

5.1.2. Build Blockchain and the SSM Component

The Blockchain will be built using. Net core and C# programming languages and their implementation of it contain some technology like cryptography, distributed ledger technology, and P2P network programming and sharing[13] .

There are several transactions that will be executed in the Blockchain and the Blockchain contains only a hash of transactions and ID of X-block that will be stored in the Google Cloud Platform (GCP).

5.2. The Smart Contract Component

The Smart Contracts component is distributed self-sufficient code that contains a set of rules for the interaction between various parties and it will be executed when met certain conditions in the Blockchain [13].

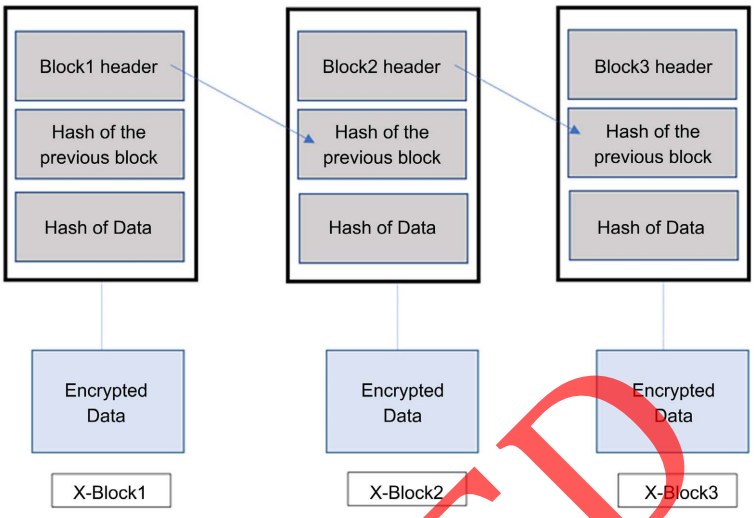

Figure 8. The data structure of blockchain and X-block.

5.2.1. The Smart Contract Mechanism

The Blockchain's Smart Contracts component will manage the IoT devices' data access policies and verify who will write and read in the Blockchain [13].

5.2.2. Build the Smart Contract Component

The Ethereum Blockchain is used to implement the Smart Contract component. The Smart Contract component's code contains the registration and suppression of both device owners and users.

Also, the code was developed in Solidity, which is an object-oriented programming language that is used to implement Smart Contracts on different Blockchain platforms [13].

6. IoT-Blockchain Platform

There are two types of platforms for IoT-based Blockchain technology, the first one is general IoT-Blockchain that will work for most IoT-Blockchain applications, and the second one is specific for SSM components, these types will be discussed smoothly below.

6.1. General IoT-Blockchain Platform

Decentralization has benefits over cloud computing as it enhances privacy and security. So, the Blockchain is a promising platform for the Internet of Things. To achieve this purpose, it is necessary to implement cloud computing and connect IoT devices with the Blockchain through a fog node [13] [14].

6.2. Platform of the SSM Component

Google Cloud Platform (GCP) is providing a set of general computing services such as Amazon AWS, Microsoft Azure, and other platforms that provide several services to developers, and the services provided by GCP are storage, management, infrastructure, and connection service between Internet of Things de-

vices, which is one of the platforms that have a strong security system, and in order to achieve the implementation of SSM component on this platform the Blockchain is linked with GCP through tools Software Development Kit (SDK) It is a set of tools that help in managing applications in the GCP platform and through which X-Bocks are sent and stored in the data store in the cloud [13] [15].

7. IoT-Blockchain Framework

Hyperledger is a Linux Foundation-hosted Blockchain platform that incorporates a modular extensible approach, interoperability, enhancing highly secure solutions, and ease of use.

The Hyperledger Blockchain frameworks have four types to support Smart Contracts which are Hyperledger Burrow, Hyperledger Fabric, Hyperledger Iroha, and Hyperledger Sawtooth.

Smart Contracts are supported differently by each framework, but they are all responsible for processing transaction requests and determining if transactions are valid by executing business logic in Smart Contracts [16].

Smart Contracts in Hyperledger Burrow is a permissioned Smart Contract machine that includes a modular Blockchain client, and a permission Smart Contract interpreter built to the Ethereum Virtual Machine's (EVM) specifications. It also includes a secure native functions framework that enables the use of native language code for improved performance and security.

In addition, Burrow's interface offers a Remote Procedure Call (RPC) that enables connecting with the node during runtime, as well as boot and runtime interfaces [16].

Smart Contracts in Hyperledger Fabric is an open-source Blockchain framework implementation called chaincode, it is made up of the system's application logic, which is the only channel that interacts with Blockchain, and the only source that generates the transactions and runs in a secured Docker container [17]. Also, the Hyperledger Fabric is written in programming languages such as Node.js, Go, and Java that implements a specific interface. It delivers high degrees of scalability, flexibility, resiliency, and confidentiality to support the implementation of different components [16] [18].

Smart Contracts in Hyperledger Iroha is documentation that is updated to reflect the latest Smart Contract functionality and provides a set of libraries, also it includes queries that make it easier for distributed ledger technologies to be integrated into IoT infrastructure [18].

Smart Contracts in Hyperledger Sawtooth is a distributed ledger that makes Smart Contracts secure, especially for enterprise use. Hyperledger Sawtooth can choose to write in seven programming languages to develop Smart Contracts in Sawtooth.

Table 3 summarizes the comparison of Smart Contracts in Hyperledger frameworks, for each framework, it will list the Smart Contract technology used and the programming language used for Smart Contracts [16].

Table 3. Smart contract in hyperledger frameworks.

Frameworks	Support Smart Contract	Programming language
Burrow	Smart Contract application engine and permissioned	Native language
Fabric	Chaincode	Node.js, Go, and Java
Iroha	Chaincode	Native language
Sawtooth	Transaction Families and distributed ledger	C++, Go, Java, JavaScript, Python, Rust, or Solidity

8. Conclusions

In conclusion, this paper described IoT based on Blockchain to enhance security by processing huge data, ensuring data integrity, increasing reliability and maintaining the privacy of digital identity without a central server or third-party intervention.

On the other hand, one of the results of combining two technologies is the emergence of several advantages that support IoT systems in terms of security and a decentralized ecosystem. Although IoT-Blockchain has unlimited advantages, it faces some challenges such as scalability and lack of skills and other challenges.

Then, this paper discussed IoT-based Blockchain architecture in general aspects as an essential five layers, and the following section is the most essential part of this paper, it demonstrates the significance of component-based development CBD in IoT-based Blockchain and how it achieves robust security and privacy goals in detail.

The platforms were presented from two aspects in general and in specific for the SSM component by Google Cloud Platform (GCP). Finally, the paper goes through the frameworks of IoT-based Blockchain that support Smart Contracts and provide services to enhance high security.

Acknowledgements

We would like to thank our supervisor Dr. Mounira Taileb for her great efforts and helped us with her tips and suggestions in writing this paper.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Atlam, H.F., Alenezi, A., Alassafi, M.O. and Wills, G.B. (2018) Blockchain with Internet of Things: Benefits, Challenges, and Future Directions. *International Journal of Intelligent Systems and Applications*, **10**, 40-48. https://doi.org/10.5815/ijisa.2018.06.05

[2] Azizi, N., Malekzadeh, H., Akhavan, P., Haass, O., Saremi, S. and Mirjalili, S. (2021) IoT-Blockchain: Harnessing the Power of Internet of Thing and Blockchain for

Smart Supply Chain. *Sensors* (*Basel*), **21**, Article 6048. https://doi.org/10.3390/s21186048

[3] Benouar, S. and Benslimane, A. (2019) Robust Blockchain for IoT Security. 2019 *IEEE Global Communications Conference* (*GLOBECOM*), Waikoloa, 9-13 December 2019, 1-6. https://doi.org/10.1109/GLOBECOM38437.2019.9013580

[4] Bhutta, M.N.M., Khwaja, A.A., Nadeem, A., *et al.* (2021) A Survey on Blockchain Technology: Evolution, Architecture and Security. *IEEE Access*, **9**, 61048-61073. https://doi.org/10.1109/ACCESS.2021.3072849

[5] Alabaa, F.A., Othman, M., Hashema, I.A.T. and Alotaibi, F. (2017) Internet of Things Security: A Survey. *Journal of Network and Computer Applications*, **88**, 10-28. https://doi.org/10.1016/j.jnca.2017.04.002

[6] Ramachandran, G.S. and Krishnamachari, B. (2018) Blockchain for the IoT: Opportunities and Challenges. Cornell University, New York. https://arxiv.org/abs/1805.02818

[7] Kazuhiro Yamashita, Y. N, Zhou, E., Pi, B.F. and Jun, S. (2019) Potential Risks of Hyperledger Fabric Smart Contracts. 2019 *IEEE International Workshop on Blockchain Oriented Software Engineering* (*IWBOSE*), Hangzhou, 24 February 2019, 1-10.

[8] Kulkarni, S. (2020) Framework for Design and Development of Blockchain Application Using Smart Contracts. Master Thesis, East Carolina University, Greenville.

[9] Lao, L., Li, Z.C., Hou, S.L., Xiao, B., Guo, S.T., and Yang, Y.Y. (2021) A Survey of IoT Applications in Blockchain Systems: Architecture, Consensus and Traffic Modeling. *ACM Computing Survey*, **53**, 1-32. https://doi.org/10.1145/3372136

[10] Miraz, M.H. (2020) Blockchain of Things (BCoT): The Fusion of Blockchain and IoT Technologies. In: S.O.I. Technology. Ed., *Advanced Applications of Blockchain Technology* (*Vol.* 60), Springer, Singapore, 141-159. https://doi.org/10.1007/978-981-13-8775-3_7

[11] Kumara, N.M. and Mallickb, P.K. (2018) Blockchain Technology for Security Issues and Challenges in IoT. *Procedia Computer Science*, **132**, 1815-1823. https://doi.org/10.1016/j.procs.2018.05.140

[12] Mitchell, N.J. and Zunnurhain, K. (2019) Google Cloud Platform Security. *Proceedings of the* 4*th ACM/IEEE Symposium on Edge Computing (SEC*' 19), New York, 7-9 November 2019, 319-322. https://doi.org/10.1145/3318216.3363371

[13] Patil, P., Sangeetha, M. and Bhaskar, V. (2020) Blockchain for IoT Access Control, Security and Privacy: A Review. *Wireless Personal Communications*, **117**, 1815-1834. https://doi.org/10.1007/s11277-020-07947-2

[14] Asuquo, P., Ogah, C., Hathal, W. and Bao, S.H. (2019) Blockchain Meets Cybersecurity: Security, Privacy, Challenges, and Opportunity. In: S.O.I. Technology. Ed., *Advanced Applications of Blockchain Technology* (*Vol.* 60), Springer, Singapore, 115-127. https://doi.org/10.1007/978-981-13-8775-3_5

[15] Wang, S., Yuan, Y., Wang, X., Li, J.J., Qin, R. and Wang, F.-Y. (2018) An Overview of Smart Contract: Architecture, Applications, and Future Trends. 2018 *IEEE Intelligent Vehicles Symposium* (*IV*), Changshu, 26-30 June 2018, 108-113. https://doi.org/10.1109/IVS.2018.8500488

[16] Cho, S. and Lee, S. (2019) Survey on the Application of BlockChain to IoT. 2019 *International Conference on Electronics, Information, and Communication* (*ICEIC*), Auckland, 22-25 January 2019, 1-2. https://doi.org/10.23919/ELINFOCOM.2019.8706369

[17] Teruel, I.C. (2020) Internet of Thingss & Statup: State of the Art and Emerging Trends. Master Thesis, Politecnico di Milano University, Milano.

[18] Bharathan, V., Bowman, M., Cole, S., Davis, S., *et al.* (2018) Hyperledger Architecture, Volume II Smart Contract. Hyperledger Blockchain Technologies for Business.