REVIEW ON BLOCKCHAIN FOR IOT SECURITY AND DATA INTEGRITY

Mujiba Shaima[1], Md Nasir Uddin Rana[1], Md Tanvir Islam[1], Norun Nabi[2]; Mazharul Islam Tusher[1], Estak Ahmed[1], Sushanta Saha[1], and Sarder Abdulla Al Shiam[3]

[1]Department of Computer Science, Monroe College, New Rochelle, New York, USA.
[2]Master of Science in Information Technology (MSIT)- Washington University of Science and Technology (WUST), Alexandria, Virginia, USA.
[3]Department of Management -Business Analytics, St Francis College, USA.

ABSTRACT

IoT, or the Internet of Things, describes a network of networked objects that are equipped with software, sensors, and other technologies to gather and share data. However, blockchain is a distributed ledger technology that makes it possible to record transactions over a network of computers in a safe, transparent, and unchangeable. The way that blockchain and IoT can enhance each other's advantages is how they are connected: Blockchain technology, with its decentralized and impenetrable ledger, offers safe and effective storage and transfer of the massive volumes of data generated by Internet of Things devices. Organizations may guarantee the security and integrity of IoT data by incorporating blockchain technology into IoT systems. This will allow for reliable and open communications and transactions between users and devices. Here, we summarize the current body of research and draw attention to the main cybersecurity issues facing blockchain-based Internet of Things platforms. These problems are divided into three primary categories: (i) security of IoT devices; (ii) security of blockchains; and (iii) integration of IoT devices with blockchain (network security). To further address a little about these issues and improve the cybersecurity of blockchain-based IoT systems, we also analysis future research directions.

KEYWORDS

IoT, Blockchain, Blockchain Layer, Hash Identification.

1. INTRODUCTION

The emergence of the Internet of Things (IoT) has revolutionized connectivity and data exchange since its conceptualization by Ashton and Gamble in 1999 [7]. This paradigm shift has led to its widespread adoption across various industries, promising enhanced efficiency and convenience through interconnected devices and networks. But as IoT ecosystems have grown exponentially, so have the security issues that threaten the security and confidentiality of the data shared across these networks.

Fundamentally, sensors integrated in devices that gather and send data to central servers or cloud computing centres enable data sharing and analysis in the Internet of Things. This connectivity creates dangers like data extraction challenges and privacy violations even if it presents until unheard-of chances for automation and creativity. The need of addressing such safety concerns is

David C. Wyld et al. (Eds): SPTM, AIS, SOENG, AMLA, NLPA, IPPR, CSIT – 2024
pp. 115-126, 2024. CS & IT - CSCP 2024 DOI: 10.5121/csit.2024.141110

increased by the forecast growth of IoT-connected devices to over 75 billion in the near future [7].

At the heart of IoT ecosystems lie fundamental components such as sensors, computing nodes, and devices, working together within a multi-layered framework encompassing the business, application, middle, network, and physical/sensor layers [3]. Modern Internet of Things networks, despite their sophisticated characteristics, have trouble allocating resources effectively and upholding strong security protocols, especially in the face of constantly changing cyberthreats [3].

The concept of Massive IoT further complicates the security landscape by envisioning networks supporting billions of connected devices, enabling innovative applications such as telepresence, autonomous driving, and biosensors. However, the sheer scale and diversity of IoT networks amplifies security concerns, underscoring the need for proactive cybersecurity measures.
In response to these challenges, emerging approaches seek to integrate cognitive technologies like artificial intelligence and machine learning with IoT environments, enhancing device capabilities and strengthening security protocols. Furthermore, trust management and data immutability emerge as crucial considerations, particularly in industries where asset tracking and privacy preservation are paramount.

Blockchain technology has emerged as a promising solution to fortify IoT security, leveraging its decentralized architecture, transparency, and cryptographic security to ensure data integrity and privacy. Blockchain-based Internet of Things solutions provide a strong foundation to reduce security risks by decentralizing data storage. However, it improves consensus processes, cryptography methods, and smart contracts [10].

Architecturally, blockchain-based IoT systems consist of distinct layers, including the device, communication, blockchain, smart contract, and application layers, each serving a unique function to ensure secure and reliable operation. Blockchain-based solutions come with their own set of difficulties that need to be managed even if they have enormous promise to solve cybersecurity issues in Internet of Things systems.

This paper aims to provide a comprehensive review of existing literature on cybersecurity challenges in blockchain-based IoT systems, categorizing challenges into three main categories and discussing potential solutions and future research directions to advance the cybersecurity of these systems [7]. Through rigorous analysis and strategic insights, this paper seeks to contribute to the ongoing discourse surrounding IoT security, fostering innovation and resilience in the face of evolving cybersecurity threats.

2. METHODOLOGY

This review paper conducts in a systematic way to thoroughly analysed the security and data integrity of blockchain for Internet of Things (IoT). The methodology comprised searching electronic databases like PubMed, IEEE Xplore, ScienceDirect, and Google Scholar for relevant material in-depth. Keywords including "Blockchain," "Internet of Things," "IoT Security," and "Data Integrity" were utilized to identify relevant peer-reviewed articles, research papers, conference proceedings, and academic publications published within a specified timeframe. Only studies meeting predefined inclusion criteria, such as relevance to the research topic and publication in reputable journals or conference proceedings, were included. Non-peer-reviewed sources, duplicate publications, and opinion pieces were excluded to maintain the integrity of the review.

Selected studies' data were gathered methodically. Then the results were analysed to reach conclusions on the use of blockchain for data integrity and Internet of Things security. The combined data were examined to find recurring themes, patterns, and gaps in the literature. The findings of the review were then synthesized and reported, providing a comprehensive overview of the current state of research in Blockchain for IoT security and data integrity [12].

3. BLOCKCHAIN TECHNOLOGY

After being first presented as an approach to prohibiting people from spending their digital currency more than once, blockchain technology has developed to be used in a variety of industries, including healthcare, logistics, and the Internet of Things. The aforementioned IoT security challenges can potentially be addressed by the blockchain. Blockchain technology can also enhance security and privacy in Internet of Things systems because of its intrinsic advantages, which include the immutability of append-only chained data, a decentralised and non-changeable ledger, transparency, and cryptographic security, among others. Several benefits of blockchain contribute to IoT system security, including:

Transparency: Since the blockchain records every transaction and makes it accessible to all users, it is a transparent technology. As a result, hackers find it more difficult to steal information or alter data. Transactions in a centralized system aren't always clear-cut, which makes it challenging to find the people who are committing fraud or altering data.

Decentralization: Blockchain is an example of a decentralized technology, meaning that no single entity controls it. Hackers find it challenging to target and launch an attack because of this. A single point of failure exists in a centralized system since all data is kept on that one server. Since data in a decentralized system is spread across several nodes, hackers have a harder time accessing all the data.

Cryptographic Methods: Blockchain protects data using cryptographic methods. Algorithms known as cryptographic techniques encrypt data, rendering it unintelligible to unauthorized users. Because of this, hackers have a harder time stealing data from the blockchain. Data is frequently stored in plain text in centralized systems, which facilitates data theft by hackers.

Consensus Mechanisms: Consensus methods are used by blockchain technology to verify transactions. Consensus methods are algorithms that guarantee that every network member agrees that a transaction is valid. Because of this, it is more difficult for hackers to control the network and authorize unauthorized transactions. Since only one party oversees verifying transactions in a centralized system, hackers have an easier time controlling the system.

Smart Contracts: Self-executing contracts that are recorded on a blockchain can be made using the blockchain. Although they are irreversible and tamper-proof, smart contracts allow for automation and the enforcement of agreements between parties. IoT system security and efficiency may increase as a result.

4. BLOCKCHAIN FRAMEWORK

Blockchain-based IoT systems can offer a strong framework for guaranteeing the integrity, privacy, and dependability of IoT data and transactions by implementing these security aspects. To comprehend the architecture and security elements of blockchain-based Internet of Things systems, it is possible to identify multiple levels [5]. These IoT system levels are depicted as follows in Figure 1:

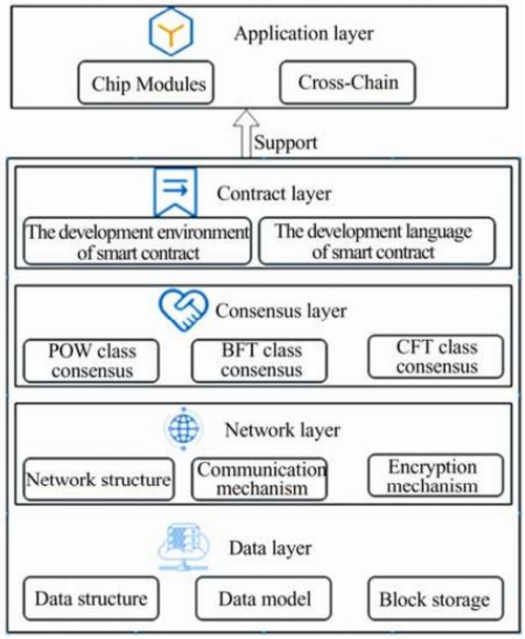

Figure 1. Blockchain Layers [14]

Data Layer: Designing data structures, grouping information, and storing it in blocks are all handled by the data layer. Data cannot be published or changed in the blocks of a blockchain network without a shared consensus process among its numerous nodes. Pointers, which indicate the position of another node, and linked lists, which show the chain of connected blocks, are the two main parts of the blockchain construction [1].

Network Layer: Intercommunication between nodes in a network is handled by the network layer by creating a secure P2P environment. To keep the blockchain network functioning, all nodes can locate, connect, synchronize, and spread with one another in this safe P2P environment. The network layer makes sure that the communications between nodes are error prone.

Blockchain Layer: The distributed ledger and related consensus processes are part of the blockchain layer, which is the fundamental part of the system. In order to guarantee the integrity and immutability of the data recorded on the blockchain, it logs and verifies transactions.

Consensus Layer: Consensus protocols, which are responsible for validating blocks, ordering new blocks according to consensus protocols, and obtaining consensus from all nodes on recently published blocks, form the foundation of blockchain architecture. They ensure that all nodes are in sync, that the network has a uniform power distribution, and that there is only one verified truth originating from all nodes [1].

Contact Layer: The basis for blockchain's programmable features is the contract layer. The runtime environment and programming language for smart contracts are presented in this work. Three groups comprise the development languages for smart contracts: (i) A scripted-based smart contract is made up of data and instructions. (ii) Cellular automata, contract language, and instructions make up a Turing-complete smart contract. (iii) One kind of verifiable contract is a smart contract. The contract syntax can be used for data storage and authorization verification, and it resembles LISP in several ways [14].

Data integrity, accountability, transparency, and interoperability can all be enhanced by blockchain-based Internet of Things systems. IoT system deployments based on blockchain, however, also bring with them particular cybersecurity issues that must be resolved. These difficulties cover topics like the integration of IoT devices with the blockchain infrastructure, security concerns with IoT devices, and blockchain security [7].

It is essential that these problems are identified and resolved in order to deploy blockchain-based IoT systems in a secure way. To overcome these obstacles and facilitate the broad deployment of blockchain-based IoT systems across several industries, ongoing research and cooperation among diverse stakeholders are required.

Our goal is to provide a thorough analysis of the body of research on cybersecurity issues with blockchain-based Internet of Things technologies. The difficulties fall into three primary groups: Three areas of concern are (i) the security of IoT devices; (ii) the security of blockchain; and (iii) the integration of blockchain security with IoT devices (network security). We also discuss the shortcomings of current options.

5. Blockchain for IoT Security

Blockchain provides security to IoT (Internet of Things) through its decentralized and immutable nature. Distributed ledger technology and cryptography are used by Blockchain to guarantee the confidentiality and integrity of data transferred between Internet of Things devices. A block, which is connected to earlier blocks to form a chain, records each transaction or data exchange. This decentralized structure eliminates the need for central authority, reducing the risk of a single point of failure or attack (figure 02).

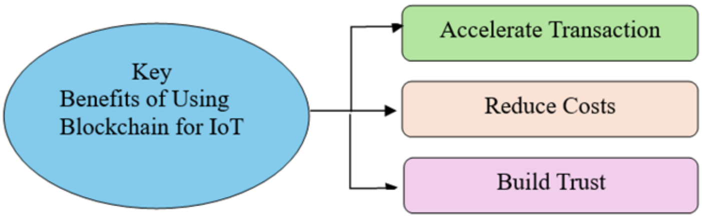

Figure 2: The blockchain and IoT [4]

Furthermore, enhancing security is the implementation of consensus techniques like Proof of Work or Proof of Stake, which guarantee that transactions are validated and accepted by network users. Moreover, the immutable nature of Blockchain prevents unauthorized tampering or modification of data, making it highly resistant to cyberattacks and unauthorized access. Overall, Blockchain enhances the security of IoT ecosystems by providing a transparent, tamper-proof, and decentralized framework for data exchange and transaction verification.

5.1. Cryptographic Techniques

- ***Encryption:*** Blockchain utilizes cryptographic algorithms to encrypt data exchanged between IoT devices, ensuring that it remains confidential and secure.
- ***Hash Functions:*** In blockchain technology, each transaction has a separate a unique cryptographic hash, which acts as a digital fingerprint. So, any kind of alteration will change its hash value. Therefore, alerting the network to tampering attempts.

- ***Digital Signatures:*** Digital signatures are used to authenticate the identity of participants in the Blockchain network. Each participant has a unique private key used to sign transactions, while public keys are used to verify signatures.

5.2. Distributed Ledger Technology (DLT)

- Every node in the decentralized network of nodes that makes up blockchain keeps a copy of the ledger. Its decentralized structure eliminates the need for a central authority and makes a single point of failure or assault less likely.
- By requiring network participants to reach a consensus, consensus algorithms like Proof of Work (PoW) and Proof of Stake (PoS) guarantee that transactions are approved and added to the Blockchain. This system keeps the ledger's integrity intact and stops fraudulent transactions [2].

5.3. Immutable Ledger

- A transaction is tamper-proof and unchangeable once it is added to the Blockchain. Since the ledger is distributed, changing historical data would require agreement from most nodes, which makes it nearly hard to change previous transactions.
- The data recorded on the Blockchain is particularly resistant to illegal modifications and hacks because of its immutability, which guarantees data integrity [2].

5.4. Smart Contracts

- In Blockchain technology smart contracts or self-executing contracts, and predetermined terms and conditions are written by itself. They enforce contracts between parties and automate the execution of transactions.
- Smart contracts help to improve security by removing middlemen and guaranteeing that transactions are carried out only when certain requirements are satisfied and reduces fraud or manipulation possibilities [2].

6. LITERATURE REVIEW

In this section, we will provide a comprehensive overview of the significant research findings and insights on blockchain security in IoT systems. We explore the different methodologies, tactics, and frameworks. These approaches that researchers have used to study the possible advantages, difficulties, and uses of blockchain technology in protecting IoT devices and networks. In addition, we emphasize the main discoveries, which involve the creation of structures, procedures, and rules for effective and protected internet of things (IoT) systems based on blockchain technology. We therefore assess performance measurements that include the ability to handle increasing demands, safeguard personal information, and establish reliability.

Li et al. (2020) conducted a thorough examination of the diverse security concerns that emerge within the framework of blockchain systems. The report highlights the susceptibility of blockchain systems to double-spending attacks as a significant security concern. Double-spending attacks occur when a person intentionally spends the same cryptocurrency twice, resulting in a loss of trust in the system. This analysis focuses on smart contracts, which are contracts that can execute themselves automatically when specific circumstances are fulfilled [9]. Nevertheless, these contracts are susceptible to a multitude of attacks, including code exploits and denial-of-service attacks. The authors explored many strategies to reduce these risks, including conducting audits and tests on smart contracts to identify weaknesses. The writers emphasised the want for additional investigation and advancement in this domain to guarantee the extensive acceptance and efficacy of blockchain technology. The article also conducted an extensive examination of the current security measures and presented solutions aimed at tackling these difficulties, rendering it a significant asset for researchers and professionals working in the domain of blockchain security.

In their research work, Dorri et al. (2017) investigated the feasibility of utilising blockchain technology to bolster security and privacy in the realm of Internet of Things (IoT) devices. The authors provided an analysis of a smart home, in which different Internet of Things (IoT) devices are interconnected and engage in communication with one another. They emphasised the security and privacy hazards linked to such gadgets, such as the possibility of unauthorised entry and data leaks. This article discusses the obstacles of applying blockchain for IoT security, including the requirement for efficient consensus processes and the possibility of higher energy usage. It also explores how blockchain technology greatly improves security and privacy in IoT devices [6].
Islam et al. (2021) conducted a thorough examination of the security concerns and obstacles that blockchain technology encounters. The writers commenced by introducing blockchain and its fundamental characteristics, including decentralisation, immutability, and transparency characteristics. Furthermore, they deliberated on the many forms of assaults that blockchain systems may encounter, including 51% attacks, double-spending attacks, and smart contract weaknesses. In addition, they showcased a range of security protections and approaches, including consensus mechanisms, encryption, and multi-signature schemes [8], that can be employed to reduce the impact of these assaults.

Raju et al. (2022) in their research paper use extensive analysis of cybersecurity concerns within the framework of Internet of Things (IoT) systems based on blockchain technology. There they emphasised the distinct security concerns presented by IoT devices, such as their constrained computational capabilities and vulnerability to physical assaults. In addition, they deliberated on the prospective advantages of employing blockchain technology to bolster security in IoT systems, such as the capacity to generate tamper-proof records and regulate access to devices and data [13].

In addition, the above authors examined other security measures, for expamle encryption, access control, and intrusion detection, that might be employed to bolster security in these systems. The report presented a comprehensive analysis of different Internet of Things (IoT) applications that utilise blockchain technology, including smart grids, healthcare, and supply chain management. It also examined the distinct security obstacles and potential advantages linked to each application.

7. BLOCKCHAIN IN DATA INTEGRITY

Blockchain technology guarantees data integrity. Integrity-security systems have characteristics that were defined by the Clark-Wilson paradigm. Properly structured transactions, job separation, audits, authentication, the principle of least privilege, objective control, and control over privilege transfers are the parts that make up this system.

7.1. Hash Identification and Data Divided into Blocks

Data from the supply chain is split up into blocks and dispersed among various devices involved in the production chain when it is integrated into a blockchain-based framework. In addition to the production data, every block in this data has a unique identification known as the "hash" and the "hash" of the block that came before it, which identifies a different portion of the same GxP data.

This "hash" identification of the block in question and the block that came before it then forms the blockchain of the data (figure 3). The hash number is modified if an unlawful change or attempted manipulation takes place in one of the blocks in this chain. As a result, any point in the network that has access to these transactions may result in inconsistent inappropriate alteration and fail to validate the newly input data.

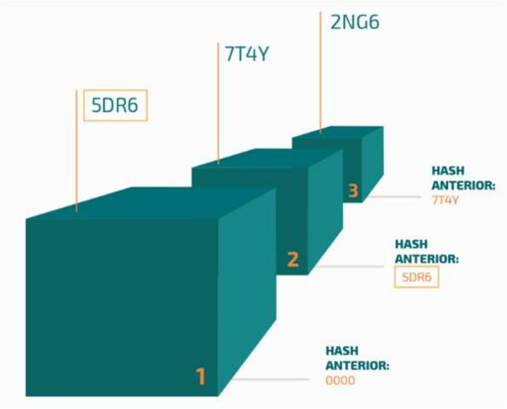

Figure 3: HASH identification [11]

7.2. Third Party Auditor

A third-party auditor is someone who has the skills and knowledge necessary to finish each auditing process. We use the third-party auditor approach to verify the data's integrity. Data integrity is achieved, and the data owner is reassured about data security by the third-party auditing architecture they have presented. The owner is aware of every resource available to him on the cloud. As such, data integrity is guaranteed by this approach for all owners of cloud resources.

The data owner takes part in the auditing process with this plan. TPA starts by using routine auditing techniques. Any changes that are discovered to the data are sent to the owner. The owner looks over the records of the auditing procedure to confirm those changes. If the owner feels that strange things have been done with his data, he can decide to have another auditor assigned by him or he can choose to independently verify his data.

As a result, the owner constantly monitors any modifications made to his personal data. The third-party auditor's response cannot go above a given threshold value. The data owner verifies any changes that fall below or are equal to this threshold. If the threshold time exceed, then the data owner is obliged to perform unforeseen audits once again.

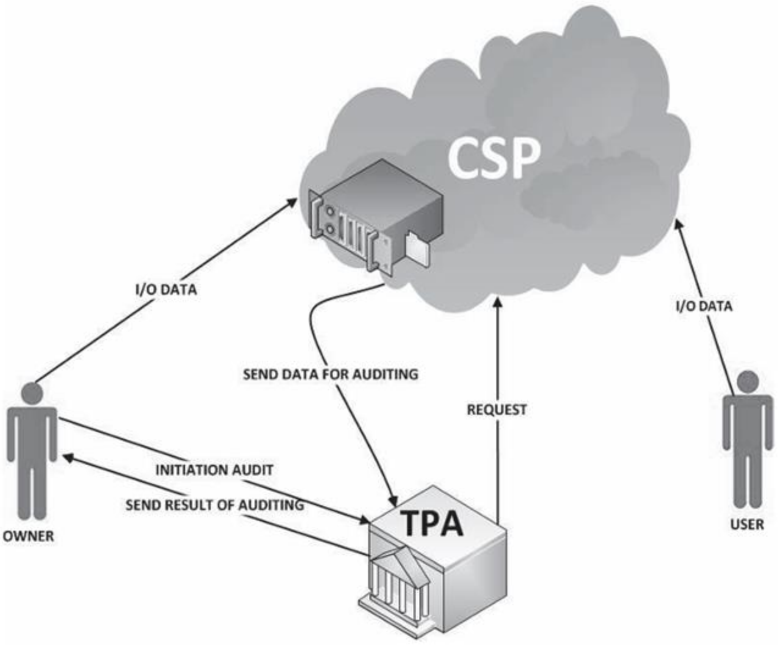

Figure 4: Third Party Method [15]

The need for a third-party communication channel and the susceptibility to "man in the middle" attacks are the disadvantages of this approach. Furthermore, the participation of a third party in data processing increases the likelihood of various hacker risks being implemented (figure 4).

7.3. Provable Data Possession (PDP) and related methods

A Provable Data Possession (PDP) technique is used to examine statistically the accuracy of data that is outsourced to cloud storage without requiring the data to be retrieved. The suggested method is meant to make sure that the server still has the original data so that it doesn't have to be retrieved from a different place. The basis of this model is probabilistic proofs, which demonstrate possession by selecting a group of blocks at random from the server.

In order to create a message that the client may use to demonstrate that the server possesses a certain block, regardless of whether the client has access to it or not, they employed an RSA-based homomorphic verifiable tag. During the pre-processing stage, the user adds metadata and edits data while simultaneously preserving the client metadata repository before submitting files to the cloud.

The user sends a request to compare the file's metadata to the client's metadata library. This request is then sent to the server to confirm that the file saved in the cloud can't be changed (figure 5).

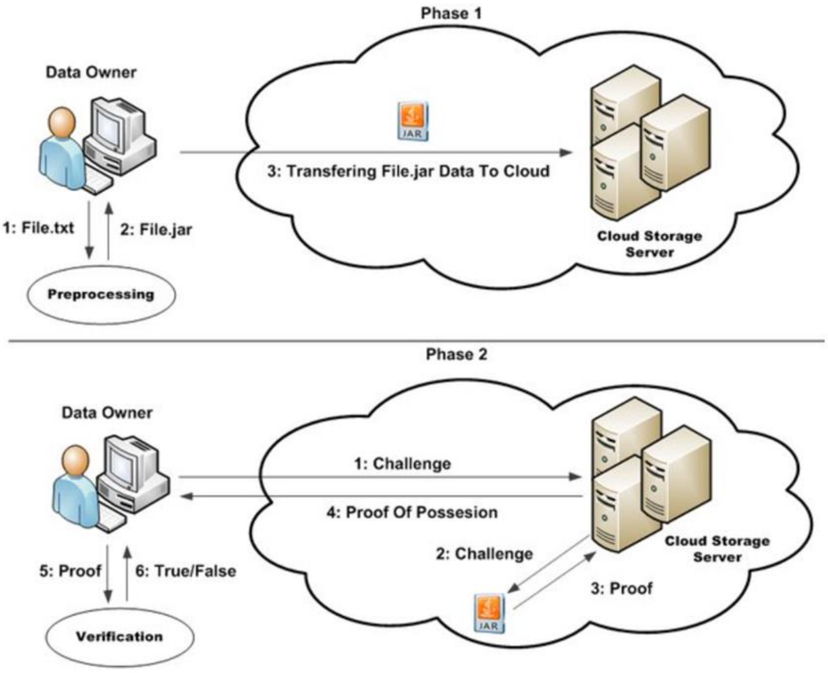

Figure 5: Provable Data Possession (PDP) preprocessing and verification phase [16]

8. Conclusion

In summary, blockchain-based Internet of Things (IoT) technologies have great potential, but addressing the related cybersecurity issues will take coordinated effort. We can create safe and dependable blockchain-based Internet of Things (IoT) systems that spur innovation and revolutionize markets by using a broad and interdisciplinary approach that comprises technological developments, operational best practices, and regulatory frameworks. To encourage people to use blockchain technology, we examine the fundamental layered architecture of blockchain technology, consensus protocols, and a range of application fields. We also document some notable advantages of blockchain adoption and explain the relationships between the many layers of technology and highlight the technical fundamentals of each layer.

Acknowledgements

We would like to express our gratitude to all those who contributed to the completion of this research paper. Special thanks are due to our families and friends for their unwavering support and understanding during this project. Their encouragement and belief in us have been a constant source of motivation.

References

[1] Altaf A, Iqbal F, Latif R, Yakubu BM, Latif S, Samiullah H. A survey of blockchain technology: architecture, applied domains, platforms, and security threats. Social Science Computer Review. 2023;41(5):1941-1962. doi:10.1177/08944393221110148

[2] Alajlan R, Alhumam N, Frikha M. Cybersecurity for blockchain-based IoT systems: a review. Applied Science. 2022;13(13):7432. doi:10.3390/app13137432

[3] Anaam E, Hasan MK, Ghazal TM, Haw SC, Alzoubi HM, Alshurideh MT. How private blockchain technology secure IoT data record. In: 2023 IEEE 2nd International Conference on AI in Cybersecurity (ICAIC). 2023;1-6. doi:10.1109/ICAIC57335.2023.10044178

[4] Banafa A. IoT and Blockchain convergence: benefits and challenges. IEEE Internet of Things Newsletter- January 2017. 2017; https://iot.ieee.org/articles-publications/newsletter/january-2017/iot-and-blockchain-convergence-benefits-and-challenges.html

[5] Bhutanadhu H. Unraveling the power of blockchain: an insight into layered architecture. Analytics Vidhya.2023; Available from: https://www.analyticsvidhya.com/blog/2023/02/unraveling-the-power-of-blockchain-an-insight-into-layered-architecture/

[6] Dorri A, Kanhere SS, Jurdak R, Gauravaram P. Blockchain for IoT security and privacy: the case study of a smart home. In: IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom workshops). 2017; p. 618-623. doi: 10.1109/PERCOMW.2017.7917634

[7] Eghmazi A, Ataei M, Landry R Jr, Chevrette G. Enhancing IoT data security: Using the blockchain to boost data integrity and privacy. MDPI. 2024;5(1):20-34. doi: 10.3390/iot5010002

[8] Islam MR, Rahman MM, Mahmud M, Rahman MA, Mohamad MHS. A review on blockchain security issues and challenges. IEEE Control and System Graduate Research Colloquium (ICSGRC). 2021; 227-232. doi: 10.1109/ICSGRC53186.2021.9515276

[9] Li X, Jiang P, Chen T, Luo X, Wen Q. A survey on the security of blockchain systems. Future generation computer systems. 2020; 107:841-853. doi: 10.1016/j.future.2017.08.020

[10] Nwosu O. The key to security: combining IoT and blockchain technology. Analytics Vidhya. 2023. Available from: https://www.analyticsvidhya.com/blog/2023/02/the-key-to-security-combining-iot-and-blockchain-technology/

[11] Rocha D. Blockchain and Data Integrity in Computer System Validation. Five Validation. [Internet]. Available from: https://fivevalidation.com/blockchain-and-data-integrity-in-computer-system-validation/

[12] Salagrama S, Bibhu V, Rana A. Blockchain Based Data Integrity Security Management. ScienceDirect. 2022; 215:331-339. https://doi.org/10.1016/j.procs.2022.12.035

[13] Raju MC, Paul KS. A comprehensive review of cyber security in blockchain-based IoT. Mathematical Statistician and Engineering Applications. 2022; 71(4):10646–10659. https://doi.org/10.17762/msea.v71i4.1957

[14] WANG Changjing, JIANG Huiwen, ZENG Jingshan, YU Min, HUANG Qing, ZUO Zhengkang. (2021). A review of blockchain layered architecture and technology application research. Wuhan University Journal of Natural Sciences. 26(5). 415-428. 10.19823/j.cnki.1007-1202.2021.0052

[15] Zikratov I, Kuzmin A, Akimenko A, Niculichev V, Yalansky L. Ensuring data integrity using blockchain technology. 2017 20th Conference of Open Innovations Association (FRUCT). 2017; 533-539. doi:10.23919/FRUCT.2017.8071359

[16] Zafar F, Khan A, Ahmed M, Iqbal M, Jabeen F. A scalable data integrity mechanism based on provable data possession and Khan JARs. KSII Transactions on Internet and Information Systems. 2016;10(6):2851-2873. doi:10.3837/tiis.2016.06.022

AUTHORS

Mujiba Shaima, MBA, MSc, was born and raised in Dhaka, Bangladesh. Currently, she is pursuing her second master's degree in computer science at Monroe College in New York. She has been employed since 2011 in Bangladesh's renowned banking and pharmaceutical industries as a software developer and quality assurance engineer.

MD NASIR UDDIN RANA completed his MBA, Master's in Agricultural Extension & Information. Currently pursuing his second master's degree in computer science at Monroe College in New York. He is a Microsoft certified professional and 14 years of professional experience to work different fields in Bangladesh. His major contribution in development sector and last working organization was Swisscontact in Bangladesh.

MD TANVIR ISLAM completed his Graduation from American International University Bangladesh in Computer Science and Software Engineering (CSSE). He was a Microsoft Student Partner (MSP) and was a windows phone app developer. Ha has 4 years of experiences in Game development and Front-End Engineering. Currently, he is doing his master's in computer science at Monroe College in New York.

NORUN NABI after graduating from Jahangirnagar University in Computer Science and Engineering, started working for a number of software companies. He is expert in Java platform and Oracle technologies to build micro-services components. He worked in the fin-tech sector while studying cryptography and application security. At present, attending Washington University of Science and Technology as an MSIT student.

MAZHARUL ISLAM TUSHER completed his Graduation from American International University of Bangladesh (AIUB) in Software Engineering (SE). He is an ambitious individual diving deeper into the realm of technology. Currently, he is pursuing master's degree in computer science at Monroe College,in New York, USA. With his dedication and thirst for knowledge, he aims to push boundaries and shape the future of AI, IOT and computer Networking.

ESTAK AHMED completed his Bachelor of Science degree in Software Engineering from Daffodil International University, Bangladesh. He was also working as a software developer in a well-known IT firm in Dhaka. Currently he is pursuing his master's degree in computer science at Monroe College in New York.

SUSHANTA SAHA completed his bachelor's degree in 2020 in Computer Science and Engineering at the American International University, Bangladesh. Now, he's delving deeper into the realm of technology as he pursues a master's in computer science at Monroe College, in New York, USA. With a passion for innovation, his research interests span Artificial Intelligence, IoT, and Computer Networking.

Sarder Abdullah Al Shiam was born and raised in Barisal, Bangladesh. He earned his Bachelor of Laws from Bangladesh University of Professionals. He was also working as a Global Graduate for a well-known multinational corporation in Dhaka. He is currently earning a master's degree in business analytics at St. Francis College in New York.