

## A Study of Blockchain-Based Internet of Things

Roheen Qamar<sup>1,\*</sup>, Baqir Ali Zardari<sup>2</sup>

<sup>1</sup>Department of Computer Science, Quaid-e-Awam University of Engineering, Science and Technology, Nawabshah, Pakistan

<sup>2</sup>Assistant Professor, Department of Information Technology, Quaid-e-Awam University of Engineering, Science and Technology, Nawabshah, Pakistan

\*Corresponding Author: Roheen Qamar

DOI: <https://doi.org/10.52866/ijcsm.2023.01.01.003>

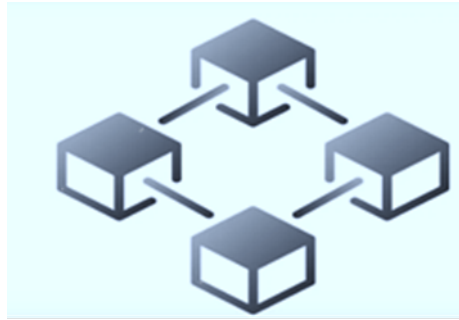
Received March 2022; Accepted October 2022; Available online October 2022

**ABSTRACT:** Blockchain and the Internet of Things (IoT), two of the most emerging technologies, are already reconfiguring our digital future, as described by the drastic change in the current network architecture. The incorporation of IoT has brought the objects around us to life, making them “smart” and capable of communicating with one another, thereby amassing massive data by consistently acquiring the physical world for analysis and intelligent action. It has made our dream of seamless integration of the digital and physical worlds a reality, altering the essence of our perception of the physical world. However, the issue with current IoT solutions is the requirement for a centrally controlled party (similar to a cloud server). This research covers the most essential implications of IoT’s most challenging scenarios, as revealed by the current studies, when connecting and communicating via the Internet. The vast amounts of generated sensitive data pose a significant risk to privacy and security; interestingly, the original architecture design calls for a decentralized system, such as the distributed or peer-to-peer (P2P) system. This scenario highlights the relevance of the blockchain, as it can offer a secure and trustworthy method of sharing information via a distributed/P2P model for achieving transparency, security, privacy, auditability, resilience, access authentication, data immutability, and so on. In this study, we explain how blockchain and IoT technologies are combined to overcome their specific shortcomings and ultimately achieve their maximum benefits. This research also discusses the technical aspects of IoT and bitcoin. We present a comprehensive overview of both technologies, including the blockchain-based IoT (BIoT) architecture and operation, and a few examples of BIoT applications and their comparison.

**Keywords:** Blockchain; Internet of Things; Blockchain and IoT Applications

### 1. INTRODUCTION

The blockchain, which was initially designed for bitcoin, is a broadly distributed and easy-to-use database. The Internet of Things (IoT) is a hub of various smart objects that communicate with one another without the need for direct social interaction. IoT permits the efficient and quick switching of records. Consequently, IoT-enabled devices have helped to improve operational efficiency, overall performance, and protection. IoT can also be regarded as a single worldwide network. Companies required to implement IoT packages forecast their sales to boom in the IoT marketplace. IoT is composed of smart devices or machines that communicate with different gadgets, machines, or infrastructure. The “things” in IoT take the form of physical and virtual items that can operate jointly in a communication network. The IoT may be static in nature [1], as presented in Figure 1.



**FIGURE 1. Blockchain Architecture**

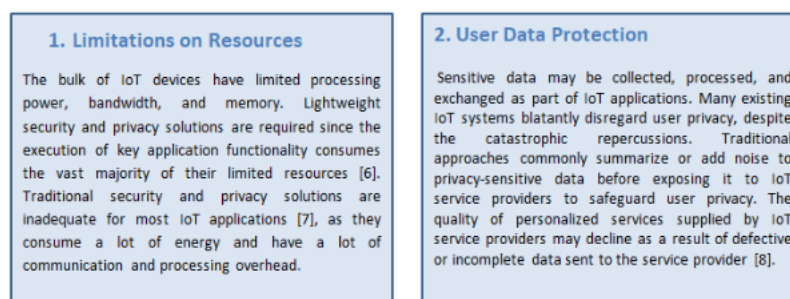
## 1.1 IOT AND ITS CHALLENGES

Certainly, IoT is no longer a mere concept nowadays, especially since it is widely used in daily living. In ordinary life, the “cellphone” is the most well-known IoT framework. The use of IoT is not restricted to smart houses. It consists of the entirety of different domains, such as commercial aspects of agriculture, public safety, and healthcare sectors. IoT is also called the Internet of Everything (IoE). Regarding the extensive variations of IoT real-global software, IoT refers to a community of more than one device that communicates with one another without requiring direct human intervention. It also allows for the green and quick transfer of data. IoT-enabled gadgets improve operational efficiency, overall performance, and safety [2].

Connected architecture, smart buildings, organization evaluations, and environmental monitoring tracking are only a few examples of commercial and consumer- and defense-related IoT activities, and they are accomplished through data collection, processing, and storage. Massive volumes of information are being disseminated nowadays. However, given the large-scale and contracted design of IoT networks, they have made IoT devices heterogeneous and diverse in terms of energy requirements. Incidentally, IoT safety and privacy remain a priority. In many cases, the data collected by IoT devices are critical for security and privacy, or it contains sensitive information for which the IoT devices are responsible. In general, devices in IoT networks are not secure, and many communities have become victims of cyberattacks [3].

## 1.2 CENTRALIZED SECURITY AND COMMUNICATION ARCHITECTURES

Security and verbal exchange architectures, including modern safety mechanisms, are generally centralized. Nonetheless, given the low-scalability and one-to-many structure of businesses and the creation of single-factor attacks (i.e., cases of IoT packages), central processes are not ideal [4]. Furthermore, when working with multiple IoT devices, dialogue styles based on centralized agents are difficult to scale. The entire cable activity is also run using cloud servers, thus creating a limitation and a fatal point [5]. Figure 2 shows an example of a formalized formal.



**FIGURE 2. Communication Architectures of IoT.**

## 2. PROS OF BITCOIN IOT TECHNOLOGIES

Figure 3 depicts the possible benefits of using cryptocurrency IoT solutions, whose development and popularity have increased in recent years.



**FIGURE 3. Advantages of Blockchain IoT.**

**Table 1. Pros of Blockchain-Based Connected Things**

|    |                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1. | <b>Tamper-Proof Tracking</b>          | Due to the hash linking of the blocks and the distributed consensus method, transactions recorded on a blockchain are tamper-proof. This gives IoT users a permanent transaction and communication history, as well as safe data capture.                                                                                                                                                                                                                                                                                                                                                              |
| 2. | <b>Distributed Design</b>             | The distributed nature of the blockchain ensures that there is no single point of failure or single point of attack in the system, and data is protected against IoT device failures or tampering. The distributed architecture also improves scalability and prevents network bottlenecks [9].                                                                                                                                                                                                                                                                                                        |
| 3. | <b>Accountability</b>                 | The time-stamped transactions on the blockchain are visible and traceable. This gives the transactions a level of accountability that they didn't have before. Participants in a network can readily verify transactions recorded on a blockchain to make sure they haven't been tampered with or excluded [10].                                                                                                                                                                                                                                                                                       |
| 4. | <b>Trustless Consensus</b>            | IoT applications entail communications and transactions between IoT systems that may or may not be trustworthy. To build confidence between untrustworthy parties, traditional designs rely on trusted intermediaries. Distributed consensus, on the other hand, is the foundation of blockchain-based IoT applications, which achieves agreement among untrusted nodes in the network and eliminates the need for trusted intermediaries [11].                                                                                                                                                        |
| 5. | <b>Privacy</b>                        | By making IoT transactions anonymous, blockchain technology has the potential to improve privacy. Public keys can be used by nodes in a blockchain network to produce pseudonymous addresses. Each single transaction is connected to a different address since each new transaction uses a separate public key, making it difficult to infer any information about the node identities merely by looking at the on-chain transactions. Other blockchain-based privacy-preserving strategies include access control, transaction mixing techniques, encryption methods, and delayed transactions [11]. |
| 6. | <b>Contracts That Are Resourceful</b> | Blockchain is a virtual area where autonomous contracts can be deployed and executed. When certain predetermined circumstances are met, smart contracts are executed without the involvement of middlemen. In IoT applications, smart contracts can be used to set the application's rules, automate operations, and enable seamless communication and transactions between IoT devices and other entities [12].                                                                                                                                                                                       |

An embedded device blockchain can record temperature, position, generated data, and status. Permanent blockchain transactions can help to arrange trustworthy data and move them rapidly and effortlessly.

### 3. BLOCKCHAINS ERA

The blockchain is not a new concept. As early as the 1990s, research on the ordering mechanism of interference timestamps has mentioned the impact to this concept. In the promotion of safe payment systems, the same notion has been extended to ledgers and transactions. Blockchain was invented by Satoshi Nakamoto, who wrote a paper about it in 2008. Since then, many software engineers, cryptographers, and scientists have collaborated to transform the blockchain into the bitcoin digital currency network [13].

#### 3.1 BLOCKCHAIN AND IOT'S SOCIAL IMPLICATIONS

The societal ramifications of blockchain and IoT are numerous. A few instances are shown in Figure 4.

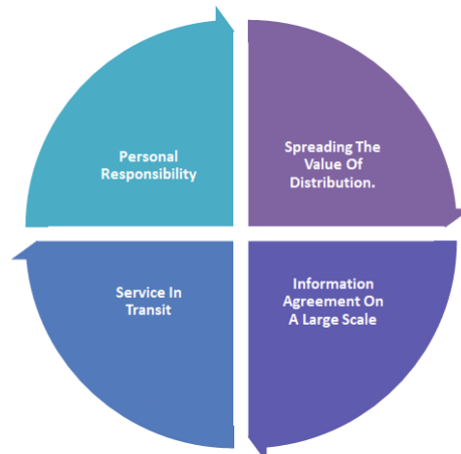
##### 1. Personal Responsibility

The accountability relies solely on the person. If you live in an open-air area, you can no longer avoid responsibilities. Your money is gone if you lose your private key [13].

##### 2. Spreading the Value of Distribution

The system is impenetrable. It is impossible to demolish the entire structure by removing a single component. The sole option is to use the network's existing value distribution. The end nodes contain all important data [13].

##### 3. Transportation Infrastructure



**FIGURE 4. A System as a Result of Blockchain and IoT**

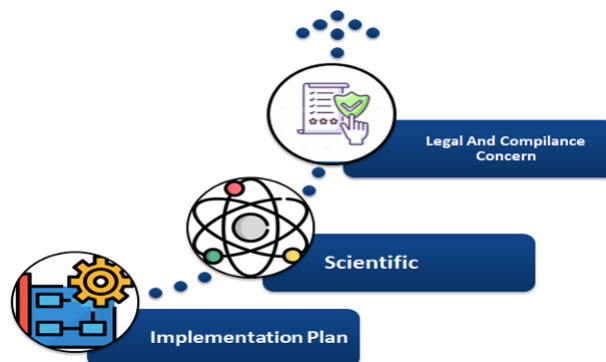
Individuals who want to go beyond the network may concentrate on providing transportation services. Money is never kept by a single node and is always transferred. The information is changed and relocated [14].

#### **4. Information Agreement on a Large Scale**

The content from a software may neither be equivalent nor redundant to the data in another software; this situation contrasts the client–server approach. As a result, a bank consortium requires a large number of middlemen who must organize a huge number of audits. The blockchain can solve this issue. In fully automating the payment and money transfer systems, the problem of the middlemen is solved by blockchain technology because it is decentralized. Besides, IoT allows all devices to be connected, whereas blockchain allows for decentralization. As a result, the two technologies can jointly make large-scale information agreement easier [14].

### **4. KEY BLOCKCHAIN AND IOT IMPEDIMENTS**

The obstacles in using the blockchain and IoT are depicted in Figure 5.



**FIGURE 5. Key Challenges in Using Blockchain and IoT.**

#### **1. Implementation Plan**

IoT and blockchain technologies are bridging the gap between disparate platforms and devices. However, devices that communicate with one another may encounter compatibility issues. We require a unified platform for all devices and a built-in technology to ensure the efficient operation of these technologies [15].

#### **2. Scientific**

Scalability, security, and storage requirements are the primary technological challenges of the blockchain and IoT technologies. Security has previously been thoroughly studied. Thus, we concentrate on the scalability problem, particularly the blockchain's inability to handle transactions in a restrictive manner. Several thousands of transactions occur per second

**Table 2. Block Benefits**

| S.no | Based On The Architecture And Functionalities Of Blockchain, It Is Clear That Blockchain Provides The Following Advantages. |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------|-----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.   | Delegation                                                                                                                  | The primary and most essential virtue of blockchain is that it runs on a distributed network, with the ledger copied across all nodes. As a result, all of blockchains additional benefits are primarily due to its decentralized character [19].                                                                                                                                                                                                                                                                                                                |
| 2.   | Integrity                                                                                                                   | Because blockchain transactions are recorded and time stamped in a decentralized ledger, they are entirely transparent. Blockchain made transaction verification even easier by employing Merkle Tree. Another key component of transparency is that the ledger can be correctly and authoritatively followed back along the chain to its point of origin [20].                                                                                                                                                                                                  |
| 3.   | Access Control                                                                                                              | Because the ledger is distributed, SPF is no longer an issue. Furthermore, by capturing 51 percent or more nodes, consensus approaches such as POW and the longest chain rule protect the blockchain network from DDoS [21].                                                                                                                                                                                                                                                                                                                                     |
| 4.   | Security And Privacy                                                                                                        | Because mathematical hashing links all time stamped records of transactions, altering one transaction in the chain invalidates not just the hash of the block to which it belongs, but also the hashes of all subsequent blocks generated after that block. A replica of the chain, on the other hand, is replicated across all network nodes, ensuring verifiability and rendering the chain totally immutable. Because existing records on the ledger cannot be removed or changed, the ledger is append-only, which adds an extra layer of immutability [22]. |
| 5.   | Charge                                                                                                                      | Deploying blockchain for large-scale applications could be more cost-effective and require less maintenance than traditional technologies, making blockchain a more cost-effective and affordable solution in the long term. Because blockchain relies on a dispersed network to function, using it on a small-scale private application could be costly. Many third-party platforms, like Ethereum, Hyperledger, and others, offer Blockchain as a Service (BaaS), many of which are cloud-based and can be used for offshoring [23].                           |

in the financial world. This situation means that the blockchain has some restrictions on security, high availability, and disk usage. These difficulties are being addressed by the researchers and are making progress [16].

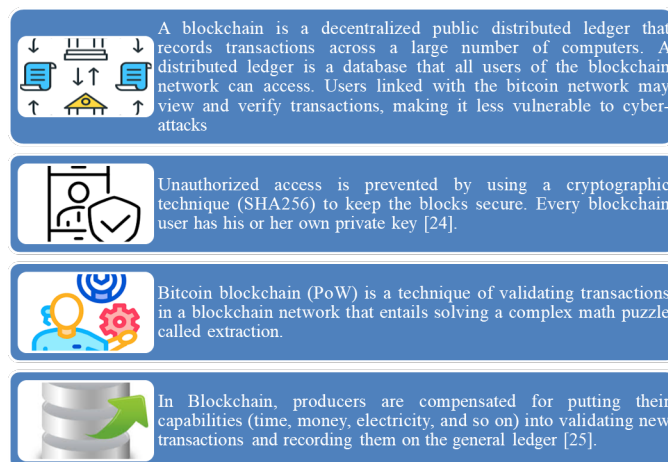
### 3. Legal and Compliance Concerns

Incorporating new technology is beneficial. However, the Internet simply lacks the ability to connect back to the physical world in a manner that it justifies the concept of IoT. An IoT is expected to encompass not only physical objects but also human activity and life. Two ethical concerns must be considered: quality control and accountability [17]. Finally, one may wonder what happens when an individual breaks a legal rule, and obtaining answers to this query is becoming more difficult. Another difficulty is the creation of an information repository. For instance, when attorneys evaluate how to secure personal data, the common question is: what will be the identity criteria? A legal and ethical question is on how to assess certain aspects in a legal and ethical perspective. According to Somov and Giaffreda [18], knowing how to establish, monitor, and manage “anything” in a framework is a legal and ethical matter.

## 5. BLOCKCHAIN

## 6. BLOCKCHAIN ESSENTIALS

The blockchain is the underlying digital infrastructure powering bitcoin and other cryptocurrencies. Its goal is to develop faster and more efficient methods of transmitting, receiving, and tracking orders by utilizing secure data. The essentiality of the blockchain is shown in Figure 6.



**FIGURE 6. Blockchain Essentials**

## 7. LITERATURE SURVEY

Novo et al. [26] evaluated the fundamentals of blockchain and IoT. To collect primary data, we examined key blockchain characteristics, such as cloud computing, intelligent compares, encryption algorithm, password protection, and others, as a way of learning how they would be applied to IoT and make it functional. We found that the blockchain is a good and acceptable paradigm for IoT and IIoT development, but certain difficulties must be handled.

Fernández-Caramés et al. [27] reviewed the security of IoT and determined the decentralized and distributed method of the blockchain, acting as a distributed ledger because all of its blocks are linked together. The blockchain can track and manage transactions and save data for billions of IoT devices. Motion time stamping, distributed consensus, data encryption, and economic incentives are used in the system. It can lower the cost, boost productivity, and addresses the problem of unsecured data storage in centralized companies.

Back et al. [28] recommended traditional centralized architectures to be transformed using a new consensus-based technique. Initially, they regarded the system as a blockchain composed of the words “block” and “chain.” By 2016, the two concepts were unified into a single word, and it led to the development of cryptocurrency.

Atlam et al. [29] used a guide to analyze blockchain and IoT technologies. They started with an overview of the fundamental structure of IoT based on the blockchain. The applications and challenges of blockchain technology were also explored. Then, the IoT system was studied by focusing on the common architecture and key characteristics. The IoT system’s numerous applications and challenges were also investigated.

Boudguiga et al. [30] demonstrated the stability of the blockchain when updating IoT devices in a network, emphasizing the blockchain’s non-variable properties. The attacker would not be able to erase a valid block that has been put to the blockchain as part of a software upgrade. By preventing threats from being installed, new software issues can also be resolved. After performing an IoT device consensus method, the modifications could be verified using the blockchain program. Furthermore, as the size of the IoT network grows, the IoT blockchain used for security to upgrade the IoT devices also becomes increasingly effective. Various gadgets could extend their lives by preventing excessive resource wastage as they would only download reliable and approved upgrades.

Dorri et al. [31] determined the importance of an IoT-optimized lightweight blockchain. As high-level calculation, complexity, and latency are often incompatible with IoT devices, the blockchain is regarded as inappropriate for IoT networks. A lightweight blockchain for IoT was created as a solution, and the overhead of the standard blockchains was removed while maintaining confidentiality. In boosting the energy efficiency, besides employing a blockchain, the proposed IoT architecture would also include a centrally managed node. Overlay networks, as opposed to sensor nodes, are constructed by central nodes with the necessary computing power and storage space to implement the public blockchain, thus ensuring end-to-end confidentiality and anonymity. They also suggested using an architecture that could utilize distributed trusts to reduce the block verification processing time. A smart home was used as a testing ground to assess how effective the proposed architecture would be. The proposed system utilized a blockchain to overcome the IoT device’s limited computing power and storage issues, but it was weak in terms of security because it relied on a central node to integrate data. The evaluation was conducted while taking into account the sensor device’s battery issues.

Sam et al. [32] proposed the creation of a lightweight blockchain by using cloud and fog computing and leveraging the blockchain as an IoT service platform. Some of the disadvantages of installing a blockchain on the IoT network include limited computer power, bandwidth, and battery capacity. Blockchain technology can be hosted on cloud and fog computing systems, but cloud and fog computing are diametrically opposed in terms of processing resources and latency. Despite the limited resources of fog computing, it has low latency. Meanwhile, cloud computing can scale incoming latency-related resource constraints. By combining blockchain technology with the aforementioned platform (i.e., cloud computing), IoT devices with limited resources can benefit from blockchain technology.

## 8. RESULTS

In 2008, the number of IoT objects surpassed the global population. Given that the IoT system’s numerous benefits, new applications and services are being produced on a daily basis. According to Statista [33], the total number of IoT devices would exceed 31 billion by the end of 2020 and even rise to nearly 75 billion by the end of 2025.

Statista [33] also reported that the global spending on blockchain solutions would increase from 4.5 billion in 2017 to 6.6 billion in 2021. The rising demand for security with digital identities and Web 3.0 is expected to drive the demand for blockchain technology in the coming years. With more firms using blockchain technology for data validation and access and identity protection measures, blockchain spending is estimated to exceed \$19 billion by 2024.

Furthermore, the IoT market is expanding at a high exponential rate. In 2015, the IoT revenue totaled USD 743 billion according to Statista. By the end of 2019, this number has risen considerably to USD 1710 billion. From 2022 to 2030, blockchain is expected to increase at an annual rate of 85.9%. Furthermore, according to Triple A and Grandview

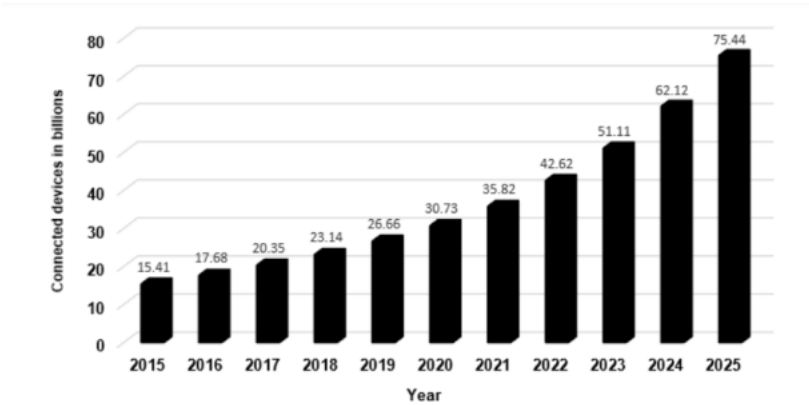


FIGURE 7. Growth projections for IoT from 2015 to 2025 [33].

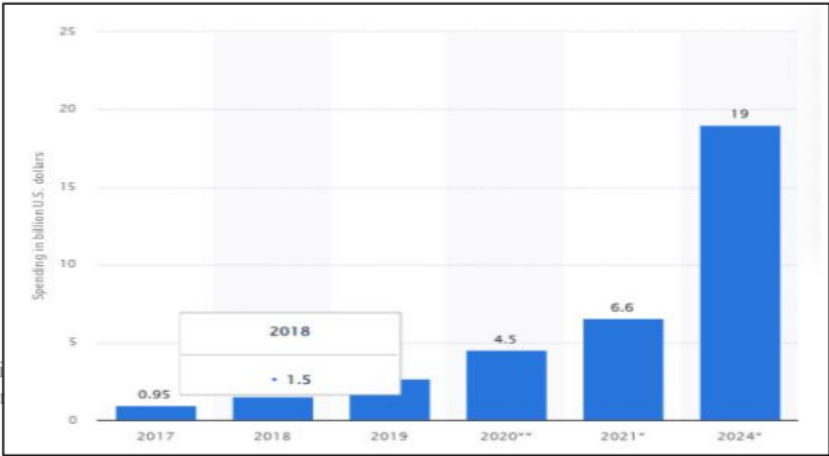


FIGURE 8. Average increase rate of blockchains [33, 34]

Research, more than 300 million people would own or use cryptocurrency in 2021, indicating their connection to a database. Grandview Research reported that the blockchain market is significantly larger than many analysts have realized. The use of contactless blockchain tickets in various events and the increase in digitization across the BPFISI industry can also boost the blockchain market. According to Grandview Research, the trade estimates by industries may increase at an annual pace of 85.9% between 2022 and 2030 to ultimately reach \$1,431.54 billion [34].

## 9. OPEN ISSUES AND FUTURE

Blockchain is an emerging and powerful technology. Blockchain-based systems offer high security, decentralization, and auditability. Despite these advantages, the adoption of blockchain technology in IIOT systems faces several challenges. In this section, we will discuss these challenges and some future research directions in the context of blockchain integration with IIoT networks.

All consensus algorithms in public and private networks require the full participation of nodes to keep a copy of all network transaction records.

It provides security, decentralization, and fault tolerance at the cost of scalability. In traditional databases, only additional storage is required in the case of growing records. Meanwhile, in blockchain-based systems, additional computational power is required to process the transactions more quickly [35].

The high performance and networking overheads of blockchain scaling are a huge issue in the implementation of digital finance and IIoT applications. The vertical scaling of blockchain is a potential research direction for addressing the scalability issue, but horizontal scaling offers a more promising solution. Accordingly, semantically independent inter-blockchain communication may be another research area.

The roles for nodes in blockchain networks were also developed [37]. In addition, IoT devices have a limited role in that they do not need to store a full copy of blockchain transactions. The derived solutions are more feasible for private blockchain implementation. Meanwhile, in public blockchains, a possible solution is to push transactions into the blockchain via the IoT gateway. In this context, computationally capable IoT gateways that can actively participate in the public blockchain will be required. Another potential future research direction is to extend the blockchain to the IoT edge. The high performance and networking overhead of the blockchain limit its use over resource-constrained IoT devices. In addressing this issue, IoT gateways can be used to push transactions through the blockchain network by using lightweight clients.

Private blockchains have a relatively high transaction rate because they do not provide fully decentralized systems. In view of providing Byzantine fault tolerance, the consensus algorithms used in private blockchains include a round of voting. This approach is not appropriate for public blockchain networks. The philosophy of the public blockchain is that all users are equal and have no governing authority. The public blockchain has latency because it uses a lottery-based consensus algorithm to create a secure and permissionless transaction platform. Therefore, consensus algorithms on blockchains create a tradeoff between decentralization and high-speed transactions. Applications beyond the cryptocurrencies need to provide users privacy while offering multiple application scenarios. Multiple blockchains are required in applications in which blockchains spread across multiple geographical locations and multiple use cases, such as IIoT. Blockchains can provide multiple IoT services by effectively communicating with one another [38].

## 10. CONCLUSION

Blockchains are thought to be a scalable technology that may be used in a wide range of areas. One of them is that the blockchain is regarded as a critical technology and capable of improving security in areas where it is lacking. Here, we examined the research patterns that link IoT and blockchain technologies to high security. Blockchain, a recently emerged technology, offers a response to problems by improving scalability, protection, reliability, visibility, and dependability. This research covers the blockchain and how it operates. The technical features of the blockchain, including related concepts, power management, reliability, anonymity, and blockchain, are explored. The economic, technological, social, and political consequences of blockchain and the IoT are also examined. There will be a slew of technological concerns as new technology emerges. As a result, the study clarifies the major problems that blockchain and IoT technologies face.

## ACKNOWLEDGEMENT

The first author would like to thank the reviewers for providing useful suggestions, allowing for the improved presentation of this paper.

## CONFLICTS OF INTEREST

The authors declare no conflict of interest.

## REFERENCES

- [1] K.-K. Choo, Z. Raymond, W. Yan, and Meng, "Blockchain in industrial IoT applications: Security and privacy advances, challenges, and opportunities," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4119–4140, 2020.
- [2] D. Bruneo, "An iot service ecosystem for smart cities: The# smartme project," *Internet of Things*, vol. 5, pp. 12–33, 2019.
- [3] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: the road ahead," *Comput. Netw.*, vol. 76, pp. 146–164, 2015.
- [4] Z. K. Zhang, M. C. Y. Cho, C. W. Wang, C. W. Hsu, C. K. Chen, and S. Shieh, "Iot security: ongoing challenges and research opportunities," *2014 IEEE 7th International Conference on Service-Oriented Computing and Applications*, pp. 230–234, 2014.
- [5] H. Birkel, E. Sebastian, and Hartmann, "Impact of IoT challenges and risks for SCM," *An International Journal*, 2019.
- [6] E. Yadav, E. A. Pooja, H. Mittal, and Yadav, "IoT: Challenges and issues in indian perspective," *2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT-SIU)*, pp. 1–5, 2018.
- [7] H. Birkel, E. Sebastian, and Hartmann, "Impact of IoT challenges and risks for SCM," *An International Journal*, 2019.
- [8] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1191–1221, 2020.
- [9] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future generation computer systems*, vol. 88, pp. 173–190, 2018.
- [10] A. Abobakr and M. A. Azer, "IoT ethics challenges and legal issues," *2017 12th International Conference on Computer Engineering and Systems (ICCES)*, pp. 233–237, 2017.
- [11] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future generation computer systems*, vol. 88, pp. 173–190, 2018.
- [12] M. Sadeeq, Mohammed, M. Nasiba, Abdulkareem, R. M. Subhi, D. M. Zeebaree, A. Ahmed, R. R. S. Sami, and Zebari, "IoT and Cloud computing issues, challenges and opportunities: A review," *Qubahan Academic Journal*, vol. 1, no. 2, pp. 1–7, 2021.
- [13] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," 2017. 464–467.
- [14] A. Gantait, J. Patra, and A. Mukherjee, "Use vehicle sensor data to execute smart transactions in Blockchain," *IBM Corp*, 2017.
- [15] M. A. Khan and K. Salah, "IoT security: review, blockchain solutions, and open challenges," *Futur. Gener. Comput. Syst.*, vol. 82, pp. 395–411, 2018.
- [16] A. Banafa, "IoT standardization and implementation challenges," *IEEE. Org Newsletter*, 2014.
- [17] M. Serrano and J. Soldatos, "IoT is more than just connecting devices: the open IoT stack explained," 2015.
- [18] A. Somov and R. Giffreda, "Powering IoT devices: technologies and opportunities," *Newsletter*, 2014.
- [19] M. Atzori, "Blockchain technology and decentralized governance: Is the state still necessary," *Available at SSRN 2709713*, 2015.
- [20] I. Zikratov, A. Kuzmin, V. Akimenko, V. Niculichev, and L. Yalansky, "Ensuring data integrity using blockchain technology," *2017 20th Conference of Open Innovations Association (FRUCT)*, pp. 534–539, 2017.
- [21] F. Di, Maesa, P. Damiano, L. Mori, and Ricci, "Blockchain based access control," in *IFIP international conference on distributed applications and interoperable systems*, pp. 206–220, Springer, 2017.
- [22] G. Karamé and S. Capkun, "Blockchain security and privacy," *IEEE Security & Privacy*, vol. 16, no. 04, pp. 11–12, 2018.
- [23] N. Kim, S. M. Ho, C. S. Kang, and Hong, "Mobile charger billing system using lightweight Blockchain," *2017 19th Asia-Pacific Network Operations and Management Symposium (APNOMS)*, pp. 374–377, 2017.
- [24] S. Gupta and K. Agarwal, "Essentials of blockchain technology for modern world applications," *Materials Today: Proceedings*, 2021.
- [25] K. A. Foster, D. Macdonald, and M. Johnson, "Blockchain and Sustainable Development Goals: From Blue Skies Estimates of Impact to Bottom-Up Essentials," in *Theories of Change*, pp. 2021–2021, Springer.
- [26] O. Novo, "Blockchain meets IoT: an architecture for scalable access management in IoT," *IEEE Internet of Things Journal*, vol. 5, no. 2, pp. 1184–1195, 2018.
- [27] T. M. Fernández-Caramés and P, "Fraga-Lamas, -A review on the use of blockchain for the internet of things," *IEEE Access*, vol. 6, pp. 32979–33001, 2018.
- [28] S. A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, and J. T. n, "Enabling Blockchain Innovations With Pegged Sidechains," 2014. <https://blockstream.com/sidechains.pdf>.
- [29] H. F. Atlam and G. B. Wills, "Technical aspects of blockchain and IoT," *Advances in computers*, vol. 115, pp. 1–39, 2019.
- [30] A. Boudguiga, "Towards better availability and .accountability for iot updates by means of a blockchain," *Security and Privacy Workshops*, 2017.
- [31] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for IoT," *Proceedings of the Second International Conference on Internet-of-Things Design and Implementation*, 2017.
- [32] M. Samaniego and R. Deters, "Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)," *IEEE*, 2016.
- [33] Statista, "Internet of Things (IoT) Connected Devices Installed Base Worldwide from," 2015. <https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/>.
- [34] H. F. Atlam, M. Ajmal, A. G. Azad, G. Alzahrani, and Wills, "A Review of Blockchain in Internet of Things and AI," *Big Data and Cognitive Computing*, vol. 4, no. 4, pp. 28–28, 2020.
- [35] S. Latif, Z. Idrees, J. Z. E. Huma, and Ahmad, "Block chain technology for the industrial Internet of Things: A comprehensive survey on security challenges, architectures, applications, and future research directions," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 11, pp. 4337–4337, 2021.
- [36] S. C. Cha, J. F. Chen, C. Su, and K. H. Yeh, "A blockchain connected gateway for BLE-based devices in the Internet of Things," *IEEE Access*, vol. 6, pp. 24639–24649, 2018.
- [37] Sawtoothhyperledgersawtooth, 2018. <https://sawtooth.hyperledger.org/docs/core/releases/latest/introduction%.html>.
- [38] "https://mybroadband.co.za/news/banking/206742-bitcoin-and-ethereum-vs-v%isa-and-paypal-transactions-per-second.html."