

Critical Concerns of Deploying Blockchain in Internet of Things Applications

Yehia Ibrahim Alzoubi ¹, Alok Mishra ², Atik Kulakli ³

¹ College of Business Administration, American University of the Middle East, Kuwait

² Faculty of Engineering, Norwegian University of Science and Technology (NTNU), Norway

³ College of Business Administration, American University of the Middle East, Kuwait

Abstract – The Internet of Things (IoT) and blockchain are both recognized as cutting-edge, popular technologies. In contrast to IoT, which pertains to the spread of linked equipment via supplying information over the Internet, blockchain offers innovative data storage and management avenues. Even as blockchain demands real-time data application and IoT specifies mechanisms to securely store and handle data overflows, a combination of the two seems promising. Blockchain, a technology created with the cryptocurrency Bitcoin, could meet the needs of the IoT. However, combining blockchain with the IoT might present a multitude of issues due to the features of blockchain and IoT technology. Although many articles have been released on the blockchain and the IoT, the concerns with this combination are still vague and dispersed. In light of this, this study seeks to give an overview of the problems that have the biggest impact on blockchain-based IoT by reviewing the pertinent peer-reviewed articles. This article also addresses some suggestions for lessening the impact of these concerns. The study considered peer-reviewed articles published within the last five years, focusing on topics related to blockchain and IoT integration. We identified 44 articles for this review.

The study's significance is that it not only expands the scholarly understanding of this complex intersection between blockchain and IoT but also provides actionable insights that can drive innovation and enhance the reliability and security of IoT ecosystems in practical settings.

Keywords – Blockchain, concerns, IoT, limitation, solution.

1. Introduction

The IoT attracts interest from scholars, professionals, and business owners due to its ability to offer unique services across various applications [1]. The IoT links many objects and gadgets to produce a particular network wherein computing, detecting, and communication tasks are dynamically handled without the need for human involvement [2]. Initially, the centralized IoT-Cloud architecture was used to accomplish such vast development [3]. However, this architecture has several flaws that render it inadequate for future demands [4]. Some of these issues include the single point of failure if the centralized server goes down, the low degree of trust among stakeholders in the cloud given that they have access to their data, and the centralized cloud server's dependency on outside parties for data collection and upkeep [3]. As a result, new, more creative solutions have to be offered. Blockchain technology, in particular, to improve data security and privacy, is one of the most appealing alternatives that many academics and companies have lately adopted [4].

Without a centralized approach, blockchain may manage, coordinate, and oversee activities conducted by multiple terminals [5]. The pair between blockchain and smart contracts protects against a single point of failure. Additionally, it makes the system more robust [6] and offers a peer-to-peer structure that eliminates the need for an intermediary mechanism, such as a third trustworthy entity [7]. Owing to the peer-to-peer nature of the network and the immutability of IoT utilizing data logs saved on blockchain, the capability of the whole network may be increased [8], [9].

DOI: 10.18421/TEM132-02

<https://doi.org/10.18421/TEM132-02>


Corresponding author: Alok Mishra,
Faculty of Engineering, Norwegian University of Science
and Technology (NTNU), Norway
Email: alok.mishra@ntnu.no

Received: 08 October 2023.

Revised: 13 February 2024.

Accepted: 04 April 2024.

Published: 28 May 2024.

 © 2024 Yehia Ibrahim Alzoubi, Alok Mishra & Atik Kulakli; published by UIKTEN. This work is licensed under the Creative Commons Attribution-NonCommercial-NoDeriv 4.0 License.

The article is published with Open Access at <https://www.temjournal.com/>

Despite all these advantages of utilizing blockchain in IoT contexts, it is still unclear how the two technologies should be combined. Because they are both still in their infancy, their advantages and disadvantages cannot be determined until the technologies are implemented into services [10], [11].

In addition, because blockchain-based IoT integration is a dynamic process affected by several interconnected elements, including blockchain, the IoT ecosystem now has more technological and functional needs [12], [13]. In light of this, it is crucial to consider the drawbacks of such technology integration. Consequently, this article seeks to offer a general overview of blockchain-based IoT application concerns and limitations by addressing the following research questions:

RQ1: What are the concerns with using blockchain in IoT applications?

RQ2: What are the literary solutions offered to address these concerns?

The main contributions to the article are as follows. There is a minimal, in-depth study on blockchain-based IoT concerns, despite the fact that blockchain has been in use for a while. This paper offers an overview of the difficulties associated with blockchain-based IoT. This work highlighted seven concerns and limitations of blockchain-based IoT applications: security, privacy, communication, capabilities, standards, blockchain platforms, and big data. Moreover, this work offers suggested solutions to the concerns and limitations presented by blockchain-based IoT. In order to identify and consider the present status of blockchain-based IoT concerns as well as possible solutions to these concerns, this article conducted an extensive review of the literature by scanning the relevant publications in the major academic databases. The remainder of the article is organized as follows. The backdrop of blockchain and IoT applications is presented in Section 2. The research questions are addressed in the third part. The paper is concluded in Section 4.

2. Background

One of the factors driving increased industrial and educational interest in blockchain is its uniqueness in providing security and privacy. This section gives some background information about the blockchain's characteristics and structure, as well as IoT applications.

2.1. Blockchain Technology

Blockchain is a decentralized and reciprocal record that maintains a list of interconnected, cryptographically protected blocks that is constantly

growing [14]. Applications built on blockchain avoid the security issues related to centralized controls [15]. All procedures are registered to protect data security and privacy [16]. The Merkle Tree, a cryptographic hash function, and a blockchain are the three technological components that make up the Bitcoin blockchain, the most popular blockchain platform, as seen in Figure 1 [17]. Mathematical algorithms called hash functions generate long strings of bits as inputs [15]. The blockchain will use the block header to monitor earlier record histories. The Merkle Tree [16] is a data structure for preserving encrypted secret keys. Blockchain may be divided into two main categories: permissioned (privately accessible) and permissionless (publicly accessible) [18], [19]. In a permissionless blockchain, all nodes are allowed to observe transactions. Each network device is capable of taking part in blockchain consensus to verify a session. The permissionless blockchain is impervious to tampering since doing so would be extremely expensive [20]. Bitcoin and Ethereum are the most well-known permissionless blockchain platforms among permissionless cryptocurrencies. On the other hand, private blockchains (e.g., multichain blockchain platforms) function even without surcharges. A private blockchain is less resistant to hacking than a public blockchain since blocks are disseminated through replica nodes [21]. Moreover, consortium blockchains are controlled by specific nodes that are not permitted to validate transactions. Anybody can view exchanges, but only a small set of nodes have the ability to actually write them [22].

2.2. Internet of Things Applications

IoT refers to a collection of objects containing software, electronics, sensors, controllers, and links that allow them to share data with each other [23]. The IoT nodes are composed of computing resources and sensor technologies that are ubiquitous in numerous sectors. Smart homes, health and medical devices, smart grids, and connected cars are a few examples of IoT [24]. IoT applications with detectors are used to track the whereabouts in real-time of medical equipment, including walkers, oxygenation concentrators, cardiac pacemakers, and others. Predictive repair is one of the IoT's finest potentials. The technology gathers relevant data from the attached car's processors, which can then be assessed in the cloud and predicted before the repair is needed [25]. Industry 4.0 may connect equipment to the Internet, providing processing experts and executives with much-needed manufacturing insight. For instance, businesses may use brake beams and radio frequency identification sensors to constantly check regions as people pass through the structure [27].

The IoT is expected to have 20 to 50 billion gadgets by 2021. More research should be carried out in this area to fully utilize the scattered architecture and worldwide capability of the IoT to embrace blockchain [26]. The concerns and limitations surrounding the use of blockchain in IoT applications highlighted in the literature are generally analyzed and summarized in this study.

However, previous studies were oriented toward IoT applications such as eHealth, smart cities, and intelligent traffic industries. More research is needed to offer a thorough knowledge of the limitations and constraints of blockchain in IoT applications because it is still in its initial phases [28].

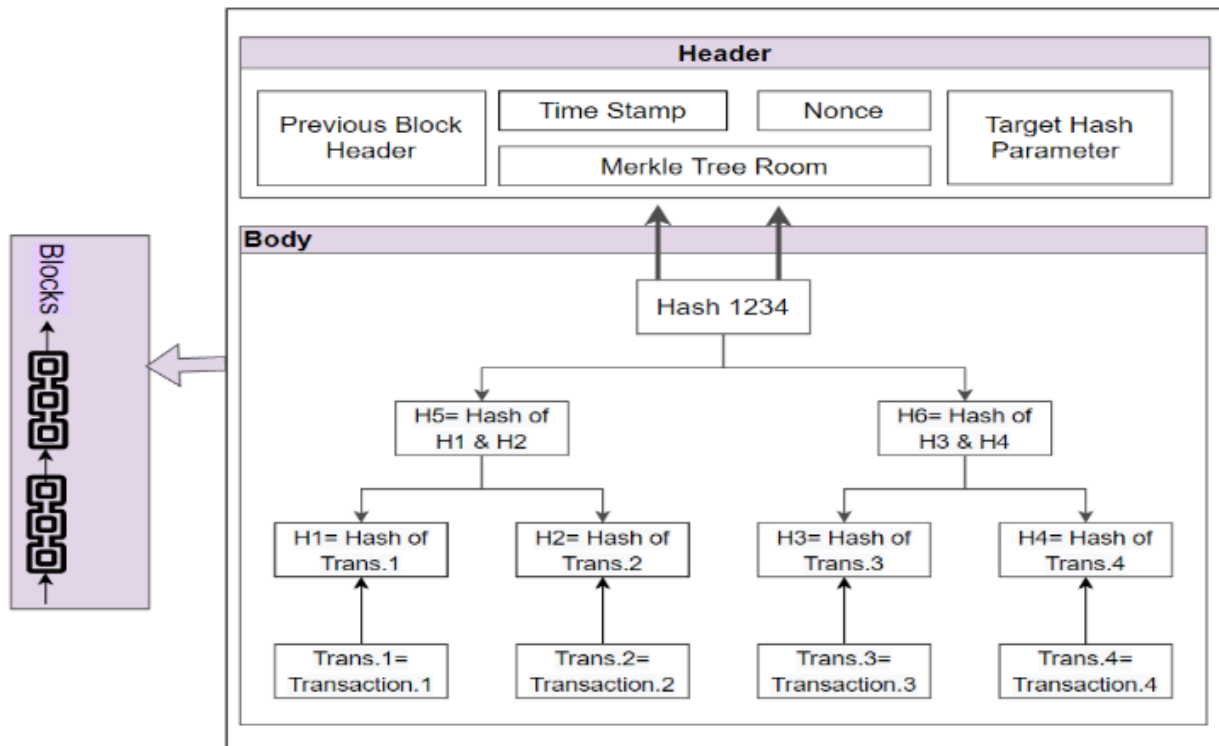


Figure 1. Bitcoin blockchain structure (based on [23])

3. RQ1, RQ2 – Limitations, Concerns, and Solutions of Deploying Blockchain in IoT Applications

This section responds to the research questions. RQ1: What are the limitations and concerns with using blockchain in IoT applications? and RQ2: What are the literary solutions offered to address these concerns and limitations? Although blockchain technology might be one of the most alluring solutions to deal with the privacy and security issues in IoT, numerous considerations are still to be considered when deploying blockchain in IoT applications, owing to the nature of these applications and blockchain technology itself [34]. This section explores these issues and possible remedies. Since much of the cited material discusses Bitcoin blockchain, most of the discussion is centered on Bitcoin blockchain concerns. In this paper, the concerns and limitations of deploying blockchain in IoT applications can be categorized into seven major categories, as shown in Table 1: security, privacy, communication, capability, standards, blockchain platforms, and big data.

We have searched all of the available literature from reputable sources, including Google Scholar, Elsevier, IEEE, Emerald, ACM, MDPI, and Springer. Through an extensive exploration of a wide range of scholarly sources and the acquisition of insights from varied viewpoints within the academic community, this thorough study sought to address the two research objectives. Boolean operators "AND" and "OR" were used in our search technique to efficiently narrow and widen the search area. For example, to get pertinent literature covering both blockchain and IoT issues, we used the query "Blockchain" AND "IoT" OR "Internet of Things". By guaranteeing that publications include both "Blockchain" AND "IoT" OR the "Internet of Things," this method allowed us to obtain full results and allowed for a more sophisticated investigation of the interrelated.

3.1. Security Concerns

The IoT is still in its infancy, and a slew of concerns need to be addressed [29]. Learning how to safeguard IoT devices is a challenging endeavor.

The development of IoT is built on the foundation of system security [30]. The consensus procedure is crucial to the security of blockchains [31]. Small blockchains with fewer users are more vulnerable to these attacks, whereas large blockchains can provide far greater security. Accordingly, the blockchain community must develop and adopt more efficient and secure consensus mechanisms [32]. On the other hand, trust must be prioritized in order to offer a safe atmosphere for all stakeholders to support this paradigm change [33]. The blockchain nodes need to be placed close to the data creator to accomplish cross-trust domain transactions while also lowering expenses [32]. On the other hand, many IoT components have limited computation and communication capacity. Maintaining the activities required by a blockchain node [34] is challenging. Thus, trust and privacy in serverless IoT devices may represent an open challenge [30]. There is currently little research on assessing node reputation in an anonymous environment using blockchain technology [35].

Developing security standards for scripting smart contracts is one area of research for blockchain-based IoT applications [16]. Despite the blockchain's intrinsic security protections, the weak link turns out to be exploitable flaws within smart contracts. The decentralized autonomous organization attack is an example of attackers taking advantage of a smart contract's flaws. The authentication code is generally static in the message authentication process.

Accordingly, the attacker can get the code using comprehensive techniques, then pretend to be the recipient and engage with the people involved [36]. In the IoT system, this behavior might leak a vast quantity of data [25]. A foundation for safe communication between internal and external entities is required. Standardized key management is necessary to safeguard security, tempering, and a robust and legal foundation for user privacy. In the future, this challenge might become a typical occurrence [26].

Due to their scalability and practicality, wireless networks have been deployed in various sectors. However, there are several security flaws in the wireless medium, including passive eavesdropping (listening to conversation without interfering with it, which makes it difficult to detect because of no discernible impact), jamming (hostile nodes intentionally disrupt networks to prevent legible communication), denial of service, and others [37]. Furthermore, managing the public and private key encryption algorithms, especially in a dispersed context, is problematic owing to the resource limits of IoT devices [38]. Moreover, many IoT systems comprise different devices' capabilities, which implies that not every device can execute the encryption method quickly, for example [29]. On the other hand, blockchain contains flaws, such as rogue nodes hijacking blockchain's communications to cause block broadcasting to be delayed [38].

Table 1. Summary of concerns and recommendations

Concern	Study	Recommendations/research directions
Security	[39]	• Establishment of a robust trust environment.
	[40]	• The needs for cryptographic development, stability, and security should be addressed.
	[25]	• More efficient and secure consensus mechanisms must be developed.
	[40]	• For auditability, contents with a public blockchain are publicly available.
	[8], [30]	• Keep data integrity in a multi-tiered architecture.
	[2], [3]	• In a public blockchain, user's data is known to everyone.
	[26]	• Small-scale integration and decentralized identifier technology development represent a big challenge.
Privacy	[3], [9]	• Pseudonymous addressing leads to privacy concerns.
	[9]	• Data privacy in tiered architecture is a challenge.
	[36]	• Off-chain solutions are still controversial.
	[16]	• Anonymity and auditability, anonymity and scalability tradeoffs.
	[40]	• More solutions and research are required.
Communication	[41]	• Design flaws in smart contract implementation, consensus protocols, and transaction capacity.
	[30]	• Blockchain needs to incorporate more reliable and faster processes for the stability of network connections.
	[37]	• Inter-blockchain communication protocols can be utilized to address the interoperability requirements.
	[25]	• The difficulty of discrepancies and trust when deploying a new contract after each upgrade.

Capability	[26]	• A smart contract cannot initiate external requests.
	[38]	• Decentralization, security of oracles, determinism, and authentication are key areas of open research.
	[42]	• Storing requirements need to be increased as a result of the storage of network-wide transactions.
	[30]	• A decentralized consensus of public blockchains reduces transaction throughput.
	[28]	• High cost and lack of standards and regulations.
	[43]	• Higher energy consumption of various consensus algorithms.
	[38], [44]	• IoT devices with limited resources have a high computational complexity requirement.
Standards	[43]	• For IoT gateways, there is a need for a lot of storage and processing power.
	[25]	• Low decentralization due to limited resources.
	[10], [28]	• Standards for developing secure smart contracts that cannot be abused for malicious purposes are required for blockchain-based IoT.
	[38]	• Competent and consistent standards and regulations are required on a global scale.
blockchain platforms	[37], [45]	• Research in this area is scarce.
	[1], [30]	• Ethereum, Hyperledger Fabric, and multichain platforms may keep leading.
	[8], [27]	• Mechanisms to validate smart contracts, model the contract conditions, and user's tools are required.
Big data	[46]	• The proxy-contact-delegation-call approach has issues with decentralization and trust.
	[14]	• Complex big data analytics methodologies on limited resources IoT devices directly are not possible.
	[21], [28]	• There is still a need to study blockchain in crowdsourcing and big data applications.
	[9]	• Providing authentication to the training data sets might be a huge difficulty.
	[38]	• Promoting users to submit their data using incentive mechanisms in order to develop machine learning models.

3.2. Privacy Concerns

Blockchain addresses are associated with the saved real identities. Users of such systems can conduct transactions across several addresses. As a result, all transaction data is kept in a single location to prevent data leakage [46]. Due to interference, such open records can leak user information and may also be used to monitor and triangulate the user's IP address [48]. Drawing conclusions from a graphical network analysis of user transactions might result in a data breach [14]. Many methods have been offered to strike a balance between privacy and accountability in the blockchain-based IoT framework [37]. The majority of proposed solutions contemplate enforcing access rules using smart contracts or inside the blockchain itself. Another interesting option for ensuring privacy in a blockchain-based environment is tiered architecture [49]. Data privacy in such a layered architecture, especially within private blockchains, is a significant difficulty [9]. Moreover, maintaining a private blockchain's data integrity while offering data seclusion is a significant research topic in a tiered

architecture [45]. As a result of the sacrifice of anonymity in blockchains to provide auditability and avoid double-spending, assured privacy remains a promising field of study for built-in privacy applications [50]. Accordingly, the ultimate answer for privacy in blockchain applications would be a kind of decentralized storage that is entirely obscured [51].

Beyond cryptocurrencies, the difficulty is to offer consumers anonymity while still enabling scalability and numerous application services. Several dispersed blockchains may communicate with each other in multiple use-case scenarios, such as the IoT, allowing for vertical and horizontal scaling [52]. On the other hand, although several techniques are now in development to solve these difficulties, off-chain alternatives, which are most typically employed in present work, are still problematic [53]. At the same time, the transaction data can be encrypted via symmetric on-chain encryption and other approaches. One of the drawbacks is that these approaches increase network latency [29].

3.3. Communication Limitations

Because peer-to-peer is the principal communication protocol in the blockchain, a faster settlement system in which numerous entities may finish transactions at the same time may be implemented. Consensus agreements may be used to seize control of the mining process. To put it another way, the blockchain will be designed to incorporate more reliable and faster processes [51]. The lack of standardization across several current platforms, diverse consensus methods, privacy methods, data models, and other factors contribute to the interoperability challenge (i.e., the restricted capacity to transfer information across multiple blockchains).

The consensus structures in public blockchains have been commonly suggested but formally shown insufficiently. Until using public blockchain consensus mechanisms, it is essential to consider the promises they have as well as their flaws. In this regard, the scientific community, in collaboration with the industry, must collaborate to validate these processes to show their validity [45]. Private blockchains, on the other hand, have implemented formal, well-known solutions, but the variety and potential of implementations are constrained due to the small number of participants in these blockchains [41]. Moreover, to establish a global security approach for IoT, the protocols used at various levels must communicate with one another by providing transition methods. An acceptable mix of security needs at each level may then be built inside the global method by taking architectural constraints into account [25].

The present mechanisms and algorithms fall well short of the blockchain expectations for IoT security. As a result, to satisfy the development of IoT security, consensus methods must be adjusted and enhanced [25]. In addition, due to the constant movement of clients, several applications in the automobile and eHealth sectors, for example, require highly adaptable mobility controls. Such applications will experience adaptability issues once they are combined with blockchain. Some publications attempted to improve mobility handling when delivering blockchain; however, this had a detrimental impact on other criteria such as latency and privacy [41]. The lack of a method for a smart contract to begin external requests is another urgent issue with the smart contract. The smart contract's sole deterministic interaction with outside real data is through event-triggered-Oracle-data feeds. Accordingly, authenticity, determinism, decentralization, security, and trust in oracles, on the other hand, are critical open research questions [37].

3.4. Capability Limitations

The utilization of high-performance computational memory placed at a blockchain node and in the blockchain network is the answer to the storage problem. Besides blockchain network nodes at a centralized place, enabling such storage through high-performance computing memory faces security and robustness problems [50]. A malfunction of the centralized memory causes the suspension of blockchain-based services. Another downside of utilizing external memory is the increased expense and collaboration required to maintain it [54]. Blockchains can leverage off-chain dispersed storage systems like Swarm and the interplanetary file system instead of centralized storage. Interplanetary file systems and Swarm, on the other hand, are open to the public, which makes them difficult to utilize. Encrypting data before uploading it to the interplanetary file system may solve this issue, but this will increase the encryption-decryption latency. Apart from that, another difficulty is the decentralized yet safe exchange of encryption-decryption keys [44].

IoT devices generally have stringent networking and processing limits, preventing them from participating in proof-of-work consensus or using blockchain-based decentralized designs [9]. Blockchain's high networking and performance costs prevent it from being used on limited IoT devices. A near-acceptable proposed approach is to use computationally powerful IoT gateways to execute end-to-end blockchain communications. Another exciting study topic is allowing IoT devices and gateways to use blockchain without requiring a centralized block validation pool [52]. Due to these applications' high networking costs and performance needs, blockchain scalability remains a major concern for its adoption in digital finance [39]. The large volume of transaction data worsens low-throughput concerns in the IoT. One potential solution for this challenge can be by scaling the blockchain vertically using a distributed database, which may make inter-blockchain communication a possible research direction since scaling the blockchain horizontally may overcome the scalability challenges in blockchain [9]. To ensure energy economy and consistency in IoT networks, a good routing architecture should be in place [26], [50].

Despite the solutions provided in the industrial IoT context, for example, vast volumes of industrial data continue to overload energy and resource-constrained equipment. As a result, developing more efficient consensus algorithms is still a work in progress [37].

On the other hand, because IoT devices cannot always provide consistent network connectivity, implementing blockchain technology in an industrial IoT environment is difficult [55]. Blockchains also have an extensive network overhead, which makes industrial IoT integration even more difficult [15]. Moreover, due to the resource limits of IoT devices and network infrastructure, the degree of decentralization feasible in existing implementations of blockchain in IoT applications is similarly constrained [56].

A multi-criteria scheduler, which aggregates computing resources using a range of approaches, is required to distribute jobs correctly to run on a collection of computer resources. Designing a multi-criteria scheduler on top of blockchain for simultaneous processing optimization, network operations, and storage is a problem [53]. Furthermore, because blockchain consumes a significant number of resources, various writers have looked at computational resource management for proof-of-work. The quantitative investigation of the resources necessary for alternative consensus protocols, on the other hand, has received little attention thus far [53].

3.5. *Standards Limitations*

Because blockchain is a decentralized technology, government rules must be followed. Bitcoin principles are still not widely acknowledged or recognized in many jurisdictions, so it is unwittingly unlawful [37]. Also, blockchain may be used for a variety of purposes other than digital money; such information must be shared internationally [10]. Moreover, deploying blockchain in an IoT context and proposing new blockchain platforms open up a world of possibilities and applications [48]. Accordingly, blockchain-based solutions are most likely hard to succeed [53]. To ensure the continued and vigorous growth of the blockchain environment, competent and consistent rules and regulations are required [45]. The blockchain ecosystem will continue to evolve safely under the supervision of effective blockchain-based regulations [50]. For example, regulations relating to cybersecurity, such as the Europe Network and Information Security Act, which was enacted by the European Commission in 2016 to improve cybersecurity throughout the EU, may be addressed in blockchain-based IoT systems [38]. Accordingly, one area of research for blockchain-based IoT applications is defining security recommendations for scripting smart contracts to avoid security vulnerabilities [10].

Despite various attempts to standardize blockchain, as described in earlier sections, these efforts appear to be simply the first step toward a successful standard integration [37]. Therefore, such standardization remains a novel concept. In IoT applications, however, data is unstructured and created by many. Directly storing this diverse data in a blockchain-based system is not an efficient solution [48]. The storage standards and data format should be sensibly studied to communicate and exchange data effortlessly among organizations. As a result, standards and guidelines for blockchain-based IoT systems are still a hot research topic [23]. It is worth noting that establishing blockchain standards should consider current industry standards, particularly those relating to the IoT. As a result, many European governments created regulations for blockchain financial transactions to boost market trust. In addition, the ISO adopted ISO/TC 307, a new standard for blockchain and distributed ledger technology [10].

3.6. *Blockchain Platforms Limitations*

No blockchain platform is flawless, and the best functionality will be followed by the platforms that remain on the market in the future. More than four platforms may become highly important in IoT applications. Ethereum and multichain are the top platforms expected to continue to be used by IoT implementations because they combine essential functionality at the moment [52]. For smart contracts to be extensively and safely accepted by customers and providers, mechanisms are required to check and ensure their correct operation. The contract's formal logic validation and its validity need to be explored in future research [50].

Furthermore, real-life contracts sometimes include non-quantifiable stipulations or circumstances. In this regard, much effort remains to be done to model the contract conditions that are representable and measurable for a machine to perform [46]. Efforts to develop techniques that enable the user to stipulate and realize smart contracts are also underway [9]. Furthermore, blockchain consumes a significant number of resources. However, a quantitative study of the resources required for various consensus protocols has received little attention thus far.

Even in the event of defects, the smart contract code is often not upgradeable. The smart contract's modified code is generally deployed with a new address, which might cause issues with inconsistency. Delegating from a proxy contract to a logic contract can help address the issue of upgradeable smart contracts [57]. The proxy contract holds the data, while the logic contract performs the

new logic. For each change, the address of the logic contract is updated in the proxy contract.

However, the proxy-contact-delegation-call approach has issues with decentralization and trust. Efforts are running partially upgradeable smart contract methods that do not enable core smart contract functionality to be updated but allow specific pieces to be upgraded [10].

3.7. Big Data Concerns

The study of IoT real-time-produced data is becoming increasingly popular. This data is typically diverse and large in volume, yet it has immense value for a business [38]. IoT big data analysis might uncover valuable and relevant information to help users make better decisions. The business demands of blockchain financial services, for example, are significant, necessitating the addition of big data and related analytic capabilities to the ledger offered by the whole blockchain [58]. A group of more than forty Japanese banks has inked a contract with Ripple to simplify the movement of payments between bank accounts and undertake real-time and low-cost transactions [48]. Another example was recently released by the Indian government by setting up a gene database system based on block linkages for 50 million people [48].

Despite these efforts, bringing traditional big data analysis to the IoT is a significant challenge due to [9], [59], [60]. 1) Resources and computational capabilities are limited for IoT devices, making it impossible to use complex big data analytics methodologies on IoT devices directly. A potential alternative is to upload the data to clouds for processing and big data analysis, although this might result in significant latency and privacy problems. 2) The digital signature of a public or private key guarantees privacy on the blockchain. However, anonymous data may make decrypting and executing big data analysis challenging and time-consuming, leading to ineffective data analytics.

4. Conclusion

It has generally been accepted that blockchains' technical traits and developmental capabilities significantly impact the real world. The blockchain has advanced swiftly since Bitcoin became well-known, which would alter the IoT ecosystem and benefit other advancements and industries. This paper assesses the current situation of blockchain-based IoT-related concerns. The proposed remedies were also covered in this paper. Despite continued efforts to create a blockchain-based IoT application that works, a number of limitations and concerns prevent

its proper implementation and limit the variety of applications that may utilize it.

We identified seven areas of concern: security, privacy, communication, capabilities, standards, blockchain platforms, and big data.

Although this study gives a general overview of these challenges and restrictions, many questions still need to be investigated and resolved. Material is sparse (e.g., outdated or inaccessible owing to the quick and constant development process), and IoT installations are still in the early phases because blockchain technology is new but still developing. Consequently, our analysis was constrained by the information and expertise we could gather from publicly available databases. Additionally, we have not performed any testing in the real world to assure that the reported transaction speed matches what is claimed in the cited research. Last but not least, the literature mostly focuses on the usage of Bitcoin as a solution for IoT applications. Although Bitcoin was the first and most widely utilized blockchain platform, some have argued that it may not be appropriate for IoT applications because of the high need for CPU power and capability. However, additional investigation is needed into this allegation.

References:

- [1]. Taloba, A. I., Elhadad, A., Rayan, A., Abd El-Aziz, R. M., Salem, M., Alzahrani, A. A., . . . Park, C. (2023). A blockchain-based hybrid platform for multimedia data processing in IoT-Healthcare. *Alexandria Engineering Journal*, 65, 263-274.
- [2]. Sharma, P., Namasudra, S., Crespo, R. G., Parra-Fuente, J., & Trivedi, M. C. (2023). EHDHE: Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain. *Information Sciences*, 629, 703-718.
- [3]. Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M., & Stiller, B. (2022). Landscape of IoT security. *Computer Science Review*, 44, 100467.
- [4]. Abed, S. e., Jaffal, R., & Mohd, B. J. (2023). A review on blockchain and iot integration from energy, security and hardware perspectives. *Wireless Personal Communications*, 129(3), 2079-2122.
- [5]. Brotsis, S., Limniotis, K., Bendiab, G., Kolokotronis, N., & Shiaeles, S. (2021). On the suitability of blockchain platforms for IoT applications: Architectures, security, privacy, and performance. *Computer Networks*, 191, 108005.
- [6]. Yazdinejad, A., Dehghantanha, A., Parizi, R. M., Srivastava, G., & Karimipour, H. (2023). Secure intelligent fuzzy blockchain framework: Effective threat detection in iot networks. *Computers in Industry*, 144, 103801.
- [7]. Dutta, P., Chavhan, R., Gowtham, P., & Singh, A. (2023). The individual and integrated impact of Blockchain and IoT on sustainable supply chains: A systematic review. *Supply Chain Forum: An International Journal*, 24(1), 103-126.

- [8]. Rahman, M. S., Chamikara, M., Khalil, I., & Bouras, A. (2022). Blockchain-of-blockchains: An interoperable blockchain platform for ensuring IoT data integrity in smart city. *Journal of Industrial Information Integration*, 30, 100408.
- [9]. Bhushan, B., Sahoo, C., Sinha, P., & Khamparia, A. (2021). Unification of blockchain and internet of things (BLoT): Requirements, working model, challenges and future directions. *Wireless Networks*, 27(1), 55-90.
- [10]. Abdi, A. I., Eassa, F. E., Jambi, K., Almarhabi, K., Khemakhem, M., Basuhail, A., & Yamin, M. (2022). Hierarchical Blockchain-Based Multi-Chaincode Access Control for Securing IoT Systems. *Electronics*, 11(5), 711.
- [11]. Bala, K., & Kaur, P. D. (2022). Changing Trends of Blockchain in IoT: Benefits and Challenges. In *12th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, IEEE. Noida, India.
- [12]. Aloqaily, M., Bouachir, O., Boukerche, A., & Al Ridhawi, I. (2021). Design guidelines for blockchain-assisted 5g-uav networks. *IEEE Network*, 35(1), 64-71.
- [13]. Alzoubi, Y. I., Al-Ahmad, A., Jaradat, A., & Osmanaj, V. H. (2021). Fog computing architecture, benefits, security, and privacy, for the internet of thing applications: An overview. *Journal of Theoretical and Applied Information Technology*, 99(2), 436-451.
- [14]. Alzoubi, Y. I., & Aljaafreh, A. (2023). Blockchain-fog computing integration applications: A systematic review. *Cybernetics and Information Technologies*, 23(1), 3-37.
- [15]. Pincheira, M., Antonini, M., & Vecchio, M. (2022). Integrating the IoT and Blockchain Technology for the Next Generation of Mining Inspection Systems. *Sensors*, 22(3), 899.
- [16]. Lin, T., Huan, Z., Shi, Y., & Yang, X. (2022). Implementation of a Smart Contract on a Consortium Blockchain for IoT Applications. *Sustainability*, 14(7), 3921.
- [17]. Lu, Y. (2018). Blockchain and the related issues: A review of current research topics. *Journal of Management Analytics*, 5(4), 231-255.
- [18]. Rizzardi, A., Sicari, S., Miorandi, D., & Coen-Porisini, A. (2022). Securing the access control policies to the Internet of Things resources through permissioned blockchain. *Concurrency and Computation: Practice and Experience*, 34(15), e6934.
- [19]. Zafar, S., Bhatti, K., Shabbir, M., Hashmat, F., & Akbar, A. (2022). Integration of blockchain and Internet of Things: challenges and solutions. *Annals of Telecommunications*, 77(1), 13-32.
- [20]. Adel, K., Elhakeem, A., & Marzouk, M. (2022). Decentralizing construction AI applications using blockchain technology. *Expert Systems with Applications*, 194, 116548.
- [21]. Sangari, M. S., & Mashatan, A. (2022). A data-driven, comparative review of the academic literature and news media on blockchain-enabled supply chain management: Trends, gaps, and research needs. *Computers in Industry*, 143, 103769.
- [22]. Alzoubi, Y. I., Gill, A., & Mishra, A. (2022). A systematic review of the purposes of blockchain and fog computing integration: Classification and open issues. *Journal of Cloud Computing*, 11(1), 1-36.
- [23]. Kumar, R. L., Khan, F., Kadry, S., & Rho, S. (2022). A Survey on blockchain for industrial Internet of Things. *Alexandria Engineering Journal*, 61(8), 6001-6022.
- [24]. Abdellatif, A. A., Samara, L., Mohamed, A., Erbad, A., Chiasserini, C. F., Guizani, M., . . . Laughton, J. (2021). MEdge-Chain: Leveraging edge computing and blockchain for efficient medical data exchange. *IEEE Internet of Things Journal*, 8(21), 15762 - 15775.
- [25]. Da Xu, L., Lu, Y., & Li, L. (2021). Embedding blockchain technology into IoT for security: A survey. *IEEE Internet of Things Journal*, 8(13), 10452 - 10473.
- [26]. Singh, S., Hosen, A. S., & Yoon, B. (2021). Blockchain security attacks, challenges, and solutions for the future distributed IoT network. *IEEE Access*, 9, 13938-13959.
- [27]. Uddin, M. A., Stranieri, A., Gondal, I., & Balasubramanian, V. (2021). A survey on the adoption of blockchain in IoT: Challenges and solutions. *Blockchain: Research and Applications*, 2(2), 100006.
- [28]. Alzoubi, Y. I., Al-Ahmad, A., Kahtan, H., & Jaradat, A. (2022). Internet of things and blockchain integration: Security, privacy, technical, and design challenges. *Future Internet*, 14(7), 216.
- [29]. Abdelmaboud, A., Ahmed, A. I. A., Abaker, M., Eisa, T. A. E., Albasheer, H., Ghorashi, S. A., & Karim, F. K. (2022). Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions. *Electronics*, 11(4), 630.
- [30]. Naseer, O., Ullah, S., & Anjum, L. (2021). Blockchain-based decentralized lightweight control access scheme for smart grids. *Arabian Journal for Science and Engineering*, 46, 8233-8243.
- [31]. Alam, S., Bhatia, S., Shuaib, M., Khubrani, M. M., Alfayez, F., Malibari, A. A., & Ahmad, S. (2023). An overview of blockchain and IoT integration for secure and reliable health records monitoring. *Sustainability*, 15(7), 5660.
- [32]. Tsang, Y., Wu, C., Ip, W., & Shiau, W.-L. (2021). Exploring the intellectual cores of the blockchain-Internet of Things (BLoT). *Journal of Enterprise Information Management*, 34(5), 1287-1317.
- [33]. Rao, A. R., & Clarke, D. (2020). Perspectives on emerging directions in using IoT devices in blockchain applications. *Internet of Things*, 10, 100079.
- [34]. Manogaran, G., Rawal, B. S., Saravanan, V., Kumar, P. M., Martínez, O. S., Crespo, R. G., . . . Krishnamoorthy, S. (2020). Blockchain based integrated security measure for reliable service delegation in 6G communication environment. *Computer Communications*, 161, 248-256.

- [35]. Kumari, A., Gupta, R., Tanwar, S., & Kumar, N. (2020). A taxonomy of blockchain-enabled softwarization for secure UAV network. *Computer Communications*, 161, 304-323.
- [36]. Wang, J., Liu, Y., Niu, S., & Song, H. (2021). Lightweight blockchain assisted secure routing of swarm UAS networking. *Computer Communications*, 165, 131-140.
- [37]. Alladi, T., Chamola, V., Parizi, R. M., & Choo, K.-K. R. (2019). Blockchain applications for industry 4.0 and industrial IoT: A review. *IEEE Access*, 7, 176935-176951.
- [38]. Al Sadawi, A., Hassan, M. S., & Ndiaye, M. (2021). A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges. *IEEE Access*, 9, 54478-54497.
- [39]. Kumar, K. D., Sudhakara, M., & Poluru, R. K. (2020). Towards the integration of blockchain and IoT for security challenges in IoT: a review. In K. C. Das, K. K. Mohbey, R. Patel, S. Prajapat, K. Saxena, D. P. Shrivastava, D. S. Sisodia, B. Tiwari, & V. Tiwari (Eds.), *Transforming Businesses with Bitcoin Mining and Blockchain Applications*, 45-67. IGI Global. Antwerp, Belgium.
- [40]. Khan, N. S., & Chishti, M. A. (2020). Security challenges in fog and IoT, blockchain technology and cell tree solutions: A review. *Scalable Computing*, 21, 515-542.
- [41]. Mistry, I., Tanwar, S., Tyagi, S., & Kumar, N. (2020). Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges. *Mechanical Systems and Signal Processing*, 135, 106382.
- [42]. Hasankhani, A., Hakimi, S. M., Shafie-khah, M., & Asadolahi, H. (2021). Blockchain technology in the future smart grids: A comprehensive review and frameworks. *International Journal of Electrical Power & Energy Systems*, 129, 106811.
- [43]. Yazdinejad, A., Parizi, R. M., Dehghantanha, A., Zhang, Q., & Choo, K.-K. R. (2020). An energy-efficient SDN controller architecture for IoT networks with blockchain-based security. *IEEE Transactions on Services Computing*, 13(4), 625-638.
- [44]. Berdik, D., Otoum, S., Schmidt, N., Porter, D., & Jararweh, Y. (2021). A survey on blockchain for information systems management and security. *Information Processing & Management*, 58(1), 102397.
- [45]. Anitha, A., & Haritha, T. (2022). The integration of blockchain with IoT in smart appliances: A systematic review. *Blockchain Technologies for Sustainable Development in Smart Cities*, 223-246.
- [46]. Pajooh, H. H., Rashid, M., Alam, F., & Demidenko, S. (2021). Hyperledger fabric blockchain for securing the edge internet of things. *Sensors*, 21(2), 359.
- [47]. Bernabe, J. B., Canovas, J. L., Hernandez-Ramos, J. L., Moreno, R. T., & Skarmeta, A. (2019). Privacy-preserving solutions for blockchain: Review and challenges. *IEEE Access*, 7, 164908-164940.
- [48]. Wang, Q., Zhu, X., Ni, Y., Gu, L., & Zhu, H. (2020). Blockchain for the IoT and industrial IoT: A review. *Internet of Things*, 10, 100081.
- [49]. Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, 82, 395-411.
- [50]. Latif, S. A., Wen, F. B. X., Iwendi, C., Li-li, F. W., Mohsin, S. M., Han, Z., & Band, S. S. (2022). AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems. *Computer Communications*, 181, 274-283.
- [51]. Abbasi, Y., & Benlahmer, H. (2022). BCSDN-IoT: Towards an IoT security architecture based on SDN and Blockchain. *International Journal of Electrical and Computer Engineering Systems*, 13(2), 155-163.
- [52]. Li, X., Lu, W., Xue, F., Wu, L., Zhao, R., Lou, J., & Xu, J. (2022). Blockchain-Enabled IoT-BIM Platform for Supply Chain Management in Modular Construction. *Journal of Construction Engineering and Management*, 148(2), 04021195.
- [53]. Yang, R., Yu, F. R., Si, P., Yang, Z., & Zhang, Y. (2019). Integrated blockchain and edge computing systems: A survey, some research issues and challenges. *IEEE Communications Surveys & Tutorials*, 21(2), 1508-1532.
- [54]. Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2021). Blockchain for healthcare data management: Opportunities, challenges, and future recommendations. *Neural Computing and Applications*, 34, 11475-11490.
- [55]. Banerjee, S., Bera, B., Das, A. K., Chattopadhyay, S., Khan, M. K., & Rodrigues, J. J. (2021). Private blockchain-envisioned multi-authority CP-ABE-based user access control scheme in IIoT. *Computer Communications*, 169, 99-113.
- [56]. Suhail, S., Hussain, R., Jurdak, R., & Hong, C. S. (2021). Trustworthy digital twins in the industrial internet of things with blockchain. *IEEE Internet Computing*, 26(3), 58 - 67.
- [57]. Miglani, A., Kumar, N., Chamola, V., & Zeadally, S. (2020). Blockchain for internet of energy management: Review, solutions, and challenges. *Computer Communications*, 151, 395-418.
- [58]. Tan, L., Shi, N., Yang, C., & Yu, K. (2020). A blockchain-based access control framework for cyber-physical-social system big data. *IEEE Access*, 8, 77215-77226.
- [59]. Xie, J., Tang, H., Huang, T., Yu, F. R., Xie, R., Liu, J., & Liu, Y. (2019). A survey of blockchain technology applied to smart cities: Research issues and challenges. *IEEE Communications Surveys & Tutorials*, 21(3), 2794-2830.
- [60]. Ferrag, M. A., Shu, L., Yang, X., Derhab, A., & Maglaras, L. (2020). Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges. *IEEE Access*, 8, 32031-32053.