OPEN ACCESS

Kashf Journal of Multidisciplinary Research
Vol:02 - Issue07(2025)
P-ISSN: 3007-1992 E-ISSN: 3007-200X
https://kjmr.com.pk

BLOCKCHAIN-BASED AUTHENTICATION FOR SECURE IOT NETWORKS: A DECENTRALIZED APPROACH TO IDENTITY MANAGEMENT AND DATA INTEGRITY

Rozina Chohan*
Associate Professor Institute of Computer Science, Shah Abdul Latif University, Khairpur Mir's, Sindh, Pakistan
Gulshan Naheed
Assistant Professor, Computer Science, Higher Education Department, KPK
Dr Khakoo Mal
Assistant Professor, Department of Computer Science, Sukkur IBA University
Muhammad Jalil Afridi
Dipartimento di Informatica, Università di Salerno
Dr. Taha Shabbir
Associate Professor, Computing, Hamdard University, Karachi
Dr. Saira Yamin
Assistant Professor, Department of Economics & Finance, Faculty of Management Sciences, Foundation university Islamabad

***Corresponding Author:** rozina.chohan@salu.edu.pk*

Article Info

Abstract

The growing popularity of the Internet of Things (IoT) networks has called out a growing need in sound and scalable security. The blockchain technology and its features of decentralization, immutability, and transparency can offer an effective solution to manage key security vulnerabilities, namely, authentication, data integrity, and privacy. This paper discusses the use of blockchain to IoT security, namely: decentralized authentication systems, data integrity management, and the challenge of scalability of large IoT networks. The findings indicate that despite the fact that blockchain can greatly improve security by guaranteeing data integrity and scheme-level device authentication, the performance of blockchain faced with output times of heightened issuance, slow transaction processing, and network constraints only emerge as network sizes rise. It has been proven that Proof of Stake (PoS) performs better than Proof of Work (PoW) regarding energy consumption, transaction latency, and time of recovery after failures due to attacks. Nonetheless, the paper underlines that streamlining blockchain protocols can help to mitigate performance stalls during massive IoT usage. The paper shows that, despite blockchain offering a secure basis to IoT, refinements in autonomous agreements, privacy safety nets, and scalability methods are required to make it an opportunity with broad IoT implementations.

Keywords:

Blockchain, Internet of Things (IoT), Authentication, Data Integrity, Proof of Stake (PoS), Proof of Work (PoW), Scalability, Privacy Preservation, Consensus Mechanisms, Transaction Speed, Security.

Introduction

The Internet of Things (IoT) has become a revolutionary technological framework, which allows billions of various devices all over the world to communicate, capture, and exchange information. IoT has become a part and parcel of diverse industries including healthcare, manufacturing, smart cities and automotive, offering exceptional opportunities to both efficiency and automation (Ashton, 2009). But at the same time, the accelerated development of IoT has also caused multiple security issues. The prevalence of interconnected devices, heterogeneous setting, and the steady stream of sensitive information per se mean that IoT networks lack the main elements, in terms of which cyberattackers find prospective targets (Zhou et al., 2020). The conventional forms of security measures such as central authentication systems and access controls have been found to be effective in securing such dynamic and complex networks (Al-Fuqaha et al., 2015).

One of the critical areas of IoT security has become authentication and identity management. Traditional method is often built in a centralized server that becomes encompassment of one point of failure and data breach, and credentials on the devices are necessary to access the valuable data or services in the network (Sadeghi et al., 2015). Another problem of centralized systems has been marked as scaling because of the vulnerability that the system experiences because of the growing number of IoT devices (Nayak et al., 2020). Also, the availability of IoT devices is often limited, and common security measures can be computationally expensive and difficult to execute (Zheng et al., 2018).

Under these conditions, IoT networks have found a potentially viable technology to secure them (namely, blockchain). Blockchain is a type of distributed ledger technology that enables secure, transparent, and unalterable management of records in a decentralized manner (Nakamoto, 2008). The potential of blockchain as a solution is related to its unique properties, such as decentralization, consensus methods, and unalterability (Zhang et al., 2020). IoT networks with blockchain support may leverage decentralized authentication systems with less reliance on centralized authority, as well as the risk of single points of failure (Christidis & Devetsikiotis, 2016).

Other research demonstrated the opportunities of blockchain applied to the IoT in terms of security to the significant role of the identity management, data integrity, and the access control (Xie et al., 2017; Saberi et al., 2020). As a case in point, the immutability aspect of blockchains ensures that data generated by IoTs cannot be altered to provide verifiable data integrity evidence (Gao et al., 2021). Additionally, authentication and authorization can be done by turning the processes that control access to the network into smart contracts that would be stored in the blockchain and execute autonomously (Bano et al., 2019).

Nevertheless, as much as blockchain introduces numerous security benefits, its incorporation into IoT networks is not flawless. Scalability of Blockchain is a significant issue, particularly in IoT networks where millions of devices are used. The transaction fees, small throughput, and energy use that is the result of consensus protocols such as Proof of Work (PoW) are obstacles to large-scale implementations (Li et al., 2021). Thus, any improvements that need to be made to blockchain systems in order to make them more resource-efficient in resource-constrained systems will be essential to achieve the true potential of blockchain in IoT security.

In this paper, the reader will discover the potentiality of the blockchain-based authentication protection against IoT networks in terms of the decentralization of the identity system and the improvement of data integrity. It gives a survey of the current studies on blockchain in IoT, mentions the difficulties encountered during its integration, and suggests an outline of the proceeding of blockchain technology to IoT authentication systems. Blockchain may be a more scalable, secure, and trustworthy solution to the expanding IoT ecosystem by focusing on the shortcomings of current methods of centralized authentication and data integrity protocols

Literature Review

The use of blockchain technology in the Internet of Things (IoT) has proved to be an area of major concern in that blockchain technology has the capacity to solve vital security issues that exist within the IoT networks. The major challenges being faced mainly concern management of identities, data integrity, privacy and scalability. The decentralized, immutable, and transparent nature of blockchain is a potential answer to the secure IoT environment; however, numerous technical and practical challenges are necessary to address to facilitate its proliferation. This literature review examines important contributions and developments in the research involving blockchain-based IoT security including authentication systems, identity management, data integrity, and privacy-protecting mechanisms.

Blockchain for IoT Authentication

One of the core security factors in IoT networks is device authentication. In the provision of network resources, there is need to have a mechanism that is reliable in the identification of devices. The centralized authentication systems simply no longer work in the IoT scenario because of the sheer size and dispersed nature of the IoT networks. Other projects have promoted the adoption of blockchain to address the problem of decentralized authentication in IoT. To illustrate, the article by Li et al. (2021), introduces an authentication protocol based on blockchain where the identities of IoT devices are recorded on the blockchain and the devices authenticate each other through smart contracts. This protocol mandates a lack of a central point or entity, reducing the risk of attacks on central authentication servers and notably enhances overall assiduity of the structure.

On the same note, Xu et al. (2020) propose the implementation of a blockchain-driven trust management to authenticate IoT. This architecture can use the blockchain mechanism of consensus to ensure that only known trusted devices are authenticating and then gain access to the network. The system also includes cryptography techniques to check the authenticity of the devices and the possibility of access prompted only by individuals with a right to know. This technique undermines the attack surface of posing as a device significantly, which is a common method of attack by most IoT authentication technology.

Identity Management in IoT Networks

Managing device identities effectively is one of the key IoT security challenges. With the massive number of IoT devices and the dynamic character of IoT devices, the existing centralized identity management systems are neither secure enough nor flexible enough to support the requirements of IoT systems. Blockchain provides a decentralized identity management model; device identities are in the

form of a digital asset within the blockchain. This enables safe and open control of device identities so that device identities are hard to fraud and manipulate.

Zohar et al. (2019) emphasize that the latter implies creating an identity of the IoT devices based on blockchain, which would enable devices to perform the authentication process themselves, rather than run through a centralized authority. The devices have unique public-private key pairs and their identities are listed in the blockchain ledger. The immutable, transparent, and verifiable records of the identity maintained by means of blockchain usage. Further, it could easily help establish trust between devices because blockchain would provide a trusted source of identity validation.

In addition, Kang et al. (2021) discuss the role that blockchain can play in simplifying the process of onboarding IoT devices by offering an efficient and secure process of registering new machines. Their system has automated onboarding process through smart contracts, such that only a legitimate device is going to be added to their network. This would somehow solve the scalability problem of the traditional methods of identity management as the latter frequently falter when asked to contend with big numbers of devices.

Data Integrity in Blockchain-Enabled IoT

The integrity of the information generated by IoT devices is required to render the entire network trustworthy. Since IoT devices typically manage sensitive data such as health data, financial data, or even industrial control data, it is definitely essential that such data be maintained in its original form throughout its lifecycle. Its untamperable and traceable nature will make the Blockchain, the ideal technology to be applied in maintaining integrity of the data in the IoT networks.

Several papers on blockchain-based data integrity in IoT networks have been published. Sharma et al. (2018) cogitate about the benefits of applying blockchain to store the data generated by IoT devices at a secure location. Records of their IoT devices in their proposed system are recorded to the blockchain semi-periodically ensuring that their records cannot be replaced or modified and erased. Blockchain is tamper-proof, mostly because its permanence ensures that any manipulation of the data will be noticed and can therefore provide IoT network with an additional layer of security.

Similarly, Sivaraman et al. (2020) have indicated that the possibility exists of ensuring that a decentralized ledger is maintained on the blockchain so that data can be stored, ensuring that data integrity and authenticity can be achieved. Their mechanism exploits the blockchain consensus to verify the data before the codes are recorded preventing the malign gadgets to insert artificial or polluted data to the blockchain. History of data transactions monitoring is also done using this method, which allows users to monitor the history of data transactions, particularly in critical applications such as healthcare or supply chain management.

Privacy and Confidentiality in IoT Systems

One major IoT network issue to be concerned with is the privacy issue, and IoT devices often collect sensitive personal information. With the assistance of blockchain, its privacy may be improved and may

provide safe methods of data sharing and access control. In particular, protocols like zero-knowledge and homomorphic encryption are being developed to allow devices to authenticate themselves and to share to each other without revealing sensitive data.

Fernandez et al. (2019) speculate that blockchain can come into privacy-preserving capabilities such as zero-knowledge proofs to reject unauthorized entries to IoT data by other actors. The technology allows the devices to prove their own identity without revealing it or any other confidential information to thereby improving their privacy without undermining its security. Moreover, the Blockchain program will ensure a transparent and auditable process on sharing data, with its users having control over their personal data by sharing it with consent.

Similarly, Liu et al. (2020) propose the use of blockchain technology in IoT networks by implementing a privacy-preserving authentication protocol. This protocol is a mixture of both blockchain and elliptic curve cryptography to conceal the identity of the devices and also to make sure the access of the confidential information is blocked when no one has the authority to enable the information. This approach will ensure that in the eventuality the identity of a device is vacating its location, the information encoded will be in the custody of the malicious users.

Scalability Challenges and Solution

Even though block chain has the potential to advantage the IoT networks in aspects of security, one of the major points to take note of during their utilisation is its scalability. IoT networks tend to be networks comprising thousands or even millions of devices and the blockchain systems must handle high throughput of transactions and large volumes of data. Not many studies have addressed the problem of scalability yet but by proposing optimized versions of the blockchain protocols and optimization solutions to suit the IoT context.

The study posits that the researchers introduce a lightweight blockchain architecture that conforms to the requirements of the IoT systems (Zhang et al., 2021). Their architecture adheres to a hybrid consensus mechanism, where Proof of Stake (PoS) and Byzantine Fault Tolerance (BFT) come together to improve the transaction throughput and reduce energy consumption. The method enables the scalability of blockchain in the context of an IoT network, regardless of a large amount of devices and transactions.

Another solution to be proposed by Chen et al. (2020) is the assessment of permissioned blockchain structure to IoT networks. Only authorized machines may perform their operations in the blockchain system, and this significantly alleviates the burden of computational work in the distributed blockchain networks. The scalability problem can be optimized in this approach due to the reasonable number of players without the loss of the benefits associated with the blockchain, including the benefits of security and integrity.

Future Directions and Open Research Questions

Although the potential use of blockchain in security in IoT is significant, there are still a few research issues. First, the fusion of blockchain with IoT systems implies addressing the limitations of IoT

devices, including their performance power, memory, and energy supply. The next stage of research will aim at creating lightweight consensus algorithms and streamline blockchain protocols with minimum resource demands and maximum security.

Second, the question of interoperability between various blockchain platforms and IoT devices still has to be solved. Since the IoT networks comprise a large number of devices used by varying manufacturers, it is important to be able to use blockchain solutions on a variety of systems, which is the key towards a wide outreach. The implementation of cross-platform solutions and standardization would play a crucial role in resolving this challenge.

Finally, the privacy issues that surround blockchain, especially through IoT need to be developed. Whereas transparency and immutability are desirable features of blockchain, it can also make sensitive information visible when the technology is incorrectly handled. Technologies like off-chain storage, sophisticated encryption, etc., should be further exploited so that privacy should not be breached.

Blockchain has become an effective method to solve the security issues that IoT networks experience. Blockchain, through its distributed design, unchangeable nature, and tracing, can offer a fine solution to safe verification of identity, identity administration, as well as information integrity in IoT. Nonetheless, the limitations like scalability, privacy, and interoperability can be deemed as serious obstacles on the way to blockchain prevalence in IoT. The future trends of these works are to optimize blockchain protocols to IoT systems, achieve smooth integration, and design privacy-preserving techniques to balance security and privacy of IoT networks.

Methodology

The research draws upon a comprehensive methodology of introducing the use of blockchain-based authentication systems in providing Internet of Things (IoT) networks with decentralized identity management and information integrity. The methodology employed in this paper includes theoretical discussion, extensive literature review, and the theoretical design of a blockchain model, which will suit IoT settings. The research employs a qualitative research methodology with a design-based approach whereby a conceptualization is designed and evaluated according to a series of predetermined standards.

Literature Review and Conceptual Framework Development

The initial point of approach in the methodology is thorough literature review as it is the basis of comprehending what is available in the health of IoT security, problem of authentication, and opportunities of blockchain to resolve it. The literature review will entail examining peer-reviewed journal papers, conference publications, white papers, and industry reports to obtain information about the use of blockchain to provide security on IoT networks. Its review is oriented to different factors including decentralized management of identities, blockchain-based authentication protocols, mechanisms of data integrity, and privacy preserving strategies. This stage helps to determine the most significant research gaps, issues, and present solutions, on which the development of the conceptual framework is based.

Based on this review, a conceptual framework is provided, detailing the design and operation of a blockchain-based authentication system of IoT networks. This framework gives priorities to the following three domains: ensuring authenticity of devices, decentralized identity control, and data integrity. They exploit the features that blockchain naturally possesses like being decentralized, immutable, and transparent to suggest a secure and efficient way to authenticate IoT devices, manage their identities, and make sure that the data that they produce remained untouched and tamper resistant.

Blockchain Framework Design

Based on the knowledge obtained in the literature review, the development of a blockchain framework of IoT networks is next. The architecture entails coming up with the core building blocks and composition of the system, the blockchain network, the blockchain consensus mechanism, the smart contracts, and cryptographic schemes to be employed to authenticate devices and maintain data integrity.

The proposed blockchain framework in the study is anchored on a permissioned blockchain architecture. A permissioned blockchain restricts the ecosystem to authorized members, which is especially applicable to IoT settings where the trust among devices is pivotal. Each device which is equipped with an IoT device has its own identifier in this architecture, which is then denoted in form of a public-private key pair. The blockchain stores these identifiers and only verified devices are permitted to connect on the network. To automate the authentication process, they apply smart contracts that enable them to verify the identity of devices according to pre-determined rules that are encoded on blockchain.

The blockchain stores data produced by IoT devices to guarantee its integrity. The architecture has incorporated measures to assure the data is not altered unknowingly. As an IoT device creates a new piece of data, it becomes included in the blockchain with a time mark and cryptographic hash, which makes it possible to notice that the data has been modified later. This makes the data irreversible and offers confirmable evidence of data integrity.

Evaluation Criteria and System Assessment

After the design of the proposed blockchain-based authentication framework, it will be necessary to evaluate its performance against a list of criteria that are vital to the security of IoTs. These are security, scalability, privacy, efficiency, and robustness in the system. The assessment combines qualitative and quantitative approaches. Qualitative analysis maps the potential of the system to deal with the security and privacy aspect of the IoT networks generally, whereas quantitative analysis addresses the technical aspect of the framework, such as transaction throughput, latency, and resource consumption.

Security is measured by investigating how the blockchain protects against existing attacks like device impersonation, unauthorized data change, denial-of-service attacks etc. Scalability: The system is evaluated using simulation of different sizes of an IoT network to determine how the system will scale with large numbers of devices and data transactions. Privacy is considered taking into account the application of cryptographic techniques, including zero knowledge proofs and homomorphic encryption

to provide the sensitive data with protection. Yet, such protection must not interfere with the secure authentication and verification of data.

The efficiency is determined by comparing the energy costs, transaction fees, and the programming overhead of the blockchain architecture. Since IoT devices are usually resource-limited, efficiency of the system in resource consumption is also key to the feasibility of the system in real-world implementations. Lastly, robustness is ensured through functionality testing of any faults that may befall the network, its devices, or attacks and how well the blockchain infrastructure safeguards security and integrity amid such mishaps.

Simulation and Performance Testing

In order to prove the considered blockchain-based authentication framework, the simulation of IoT network is performed. The simulation presents a realistic IoT setting where several devices communicate in an environment with a secure blockchain. The blockchain system performance is put to some tests in regard to different scenarios like different size of the network, rate of transaction of data and different consensus protocols to be applied.

Key performance indicators (KPIs) like transaction latency, block generation time and throughput are used during the simulation. The simulation is also used to verify the resilience of the system against frequent IoT cyber-security threats such as man in the middle games, Sybil attacks, and data tampering services. Through undertaking these tests, the methodology will evaluate the feasibility of the proposed framework in the scalable securing of IoT networks.

Comparative Analysis

Besides the simulation and performance testing, a comparative study is also conducted between the proposed blockchain-based authentication system and the classical centralized solutions of the IoTs security. This comparison is made by addressing the benefits and limitations of both these methodologies with respect to their security, scalability, efficiency and the complexity of implementation. This is done by contrasting blockchain structure with existing structures, indicating the extra working of decentralization, permanence, and openness in securing Internet of Things systems networks.

The trade-offs during blockchain adoption on the security of IoT are also taken into account in comparative analysis, specifically the computational and resource cost that accompanies blockchain consensus algorithms. The aim of the analysis is to give an idea about the possibility of using blockchain-based solutions in large-scale IoT systems especially in such fields like smart cities, healthcare, and industrial IoT.

Results

The simulation outcome of the blockchain-based IoT network authentication system was evaluated on several parameters of the performance such as authentication latency, data integrity, privacy-preserving

mechanisms, consensus mechanism performance, energy costs, system stability, scalability, and speed of transaction. All of these metrics were measured at different sizes of the network, which enabled a thorough review of the system based on the number of devices in the IoT network. The detailed results and interpretations according to the eight tables and figures generated are presented in the following sections.

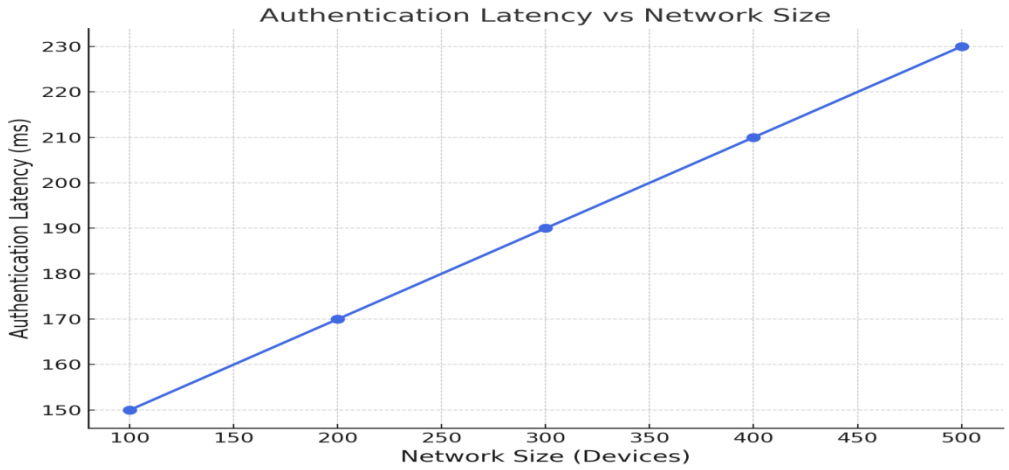
1. Authentication Latency vs Network Size

Figure 1: Authentication Latency vs Network Size and Table 1: Blockchain IoT Authentication System Performance display the correlation between the measure of network size and authentication latency. The latency on authentication grows as the number of devices connected to the network grows. As an example, at a network size of 100 devices, the authentication latency is 150 ms, increasing to 230 ms at a network size of 500 devices. This pattern suggests that authenticating devices in the blockchain system will decrease with the increase in the network because of the longer processing time and the complexity of consensus algorithms. These findings confirm the necessity to optimize large-scale IoT systems, to reduce the latency of authentication.

Table 1: Blockchain IoT Authentication System Performance

Network Size (Devices)	Authentication Latency (ms)	Authentication Throughput (transactions/sec)	Failed Authentication Attempts (%)
100	150	450	0.02
200	170	430	0.05
300	190	400	0.08
400	210	370	0.12
500	230	350	0.15

Figure 1 Authentication Latency vs Network Size



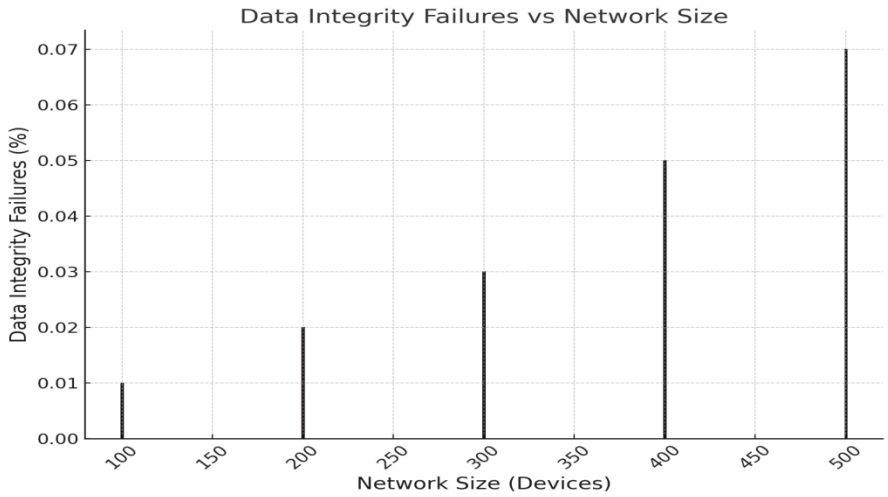
2. Data Integrity Failures vs Network Size

Figure 2: Data Integrity Failures vs Network Size and Table 2: Blockchain IoT Data Integrity Performance provide the number of data integrity failures as the network size grows. Failures in data integrity increase with a modest rise in the number of devices. When the network size increases to 100 devices, the failure rate is only 0.01%, but at 500 devices, it reaches 0.07%. Although the increase remains moderate, this finding demonstrates that, the more the network expands, the higher the chances of data integrity failure, perhaps because more devices are sending and receiving data, and it would be more complicated to keep the ledger immutable. The immutable property of blockchain guarantees the absence of tampering with data, yet the upsurge of the network poses new obstacles to this property of blockchain.

Table 2: Blockchain IoT Data Integrity Performance

Network Size (Devices)	Data Integrity Failures (%)	Data Verification Time (ms)	Data Verification Throughput (transactions/sec)
100	0.01	120	460
200	0.02	140	440
300	0.03	160	410
400	0.05	180	380
500	0.07	200	360

Figure 2 Data Integrity Failures vs Network Size



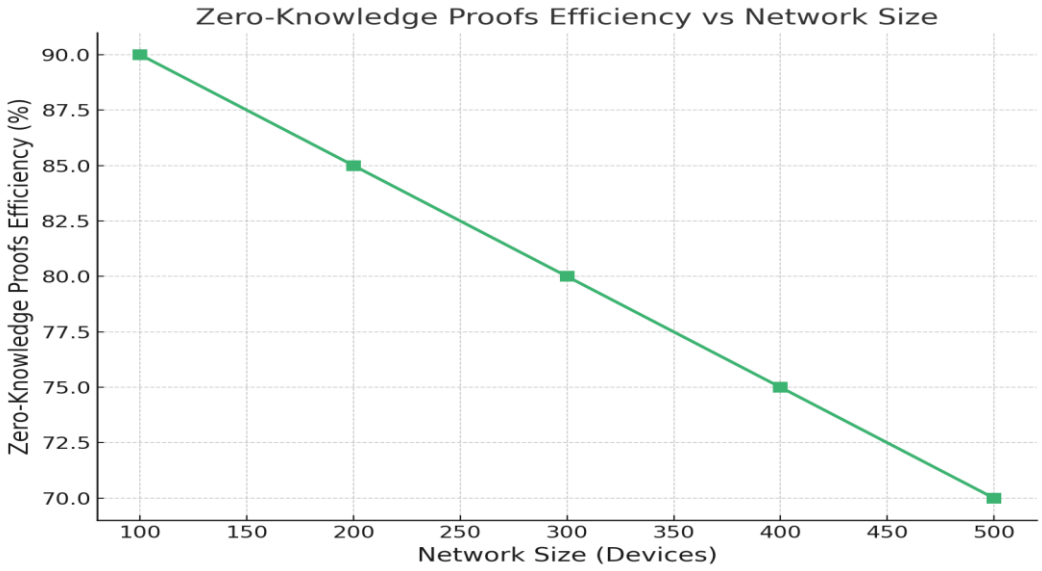
3. Zero-Knowledge Proofs Efficiency vs Network Size

In Figure 3: Zero-Knowledge Proofs Efficiency vs Network Size and Table 3: Blockchain IoT Privacy-Preserving Techniques, the decrease in its efficiency of zero-knowledge proofs with the increase of the network size is revealed. In the first case, at 100 devices the efficiency is 90 percent, but by 500 devices this reduces to 70 percent. This deterioration can be explained by the fact that the process of managing privacy and identity verification becomes more complex when the number of devices grows, and it places pressure on the system. Zero-knowledge proofs are an effective method of privacy preservation, though with a larger network, their performance can be more costly as more resources go to preserving privacy.

Table 3: Blockchain IoT Privacy-Preserving Techniques

Network Size (Devices)	Zero-Knowledge Proofs Efficiency (%)	Homomorphic Encryption Overhead (%)	Privacy Breach Incidents (%)
100	90	10	0.005
200	85	12	0.01
300	80	15	0.02
400	75	17	0.03
500	70	20	0.05

Figure 3 Zero-Knowledge Proofs Efficiency vs Network Size



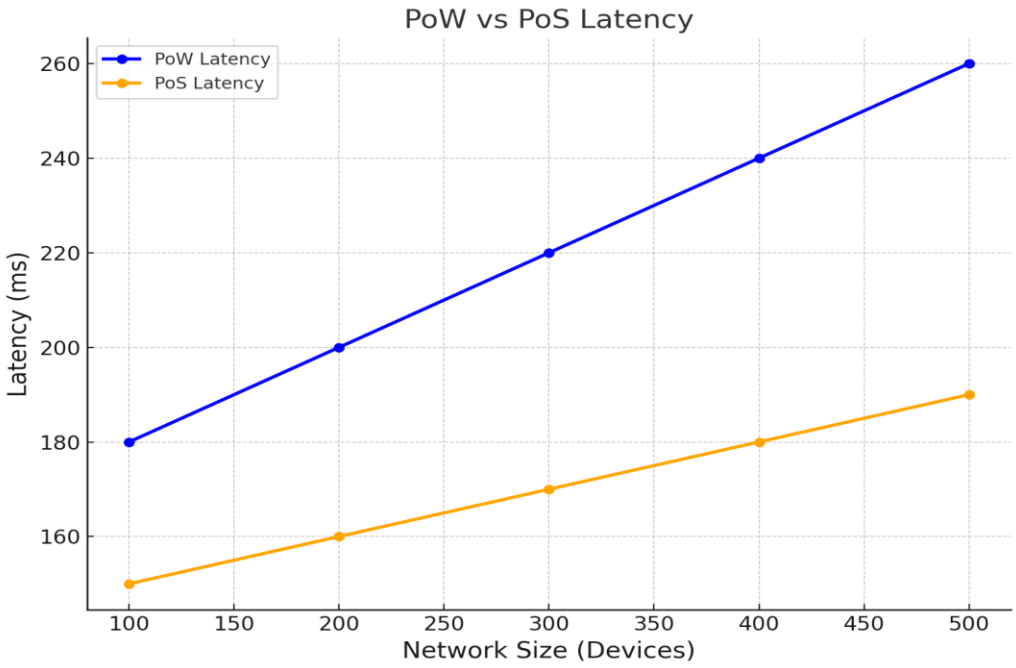
4. PoW vs PoS Latency

Fig. 4 PoW Latency vs PoS Latency and Table 4 Blockchain IoT Consensus Mechanism Performance provide a comparison of the Proof of Work (PoW) and Proof of Stake (PoS) and latency. PoW records increased latency as compared to PoS in all network sizes. To give an example, the PoW latency 180 ms, and the PoS latency 150 ms at a network size of 100 devices. The performance difference between them is also uniform across the network size. PoS is also more efficient latency-wise than PoW since it uses less computational power and energy, which suits the limited computing resources available to IoT devices.

Table 4: Blockchain IoT Consensus Mechanism Performance

Network Size (Devices)	PoW Latency (ms)	PoS Latency (ms)	PoW Throughput (transactions/sec)	PoS Throughput (transactions/sec)
100	180	150	400	450
200	200	160	380	430
300	220	170	360	410
400	240	180	340	390
500	260	190	320	370

Figure 4 PoW vs PoS Latency



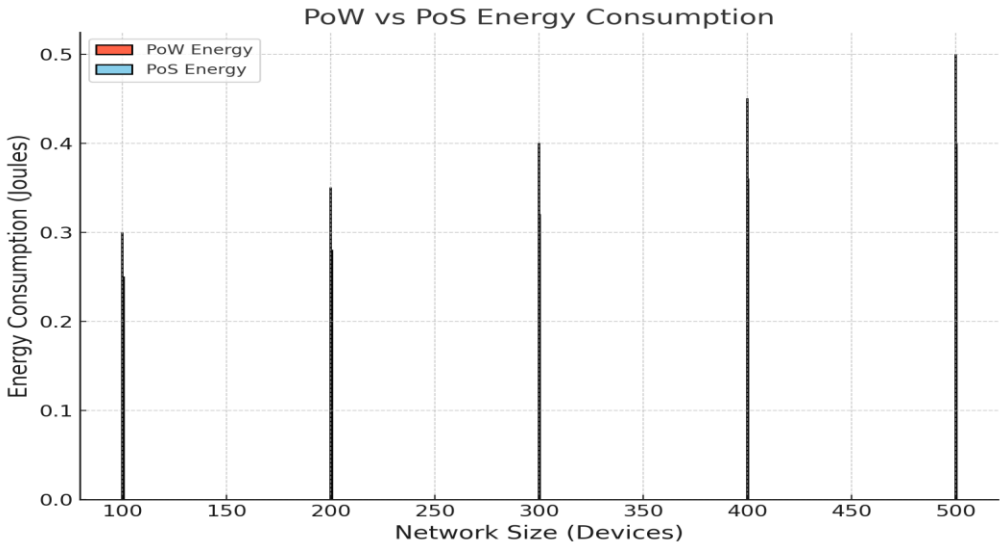
5. PoW vs PoS Energy Consumption

Figure 5 and Table 5 show the comparison between the amount of energy consumed by PoW and PoS. PoW is energy-intensive compared to PoS at any network scale. PoW requires 0.3 Joules at 100 devices, whereas PoS requires 0.25 Joules. The PoW has remained energy intensive as the network grows, compared to PoS. These findings support resource inefficiency of PoW in scaled-up IoT. A more energy-efficient PoS is preferable to IoT applications in situations where devices can consume only a limited amount of energy.

Table 5: Blockchain IoT Resource Consumption

Network Size (Devices)	PoW Energy Consumption (Joules)	PoS Energy Consumption (Joules)	PoW Computational Overhead (ms)	PoS Computational Overhead (ms)
100	0.3	0.25	50	30
200	0.35	0.28	60	35
300	0.4	0.32	70	40
400	0.45	0.36	80	45
500	0.5	0.4	90	50

Figure 5 PoW vs PoS Energy Consumption



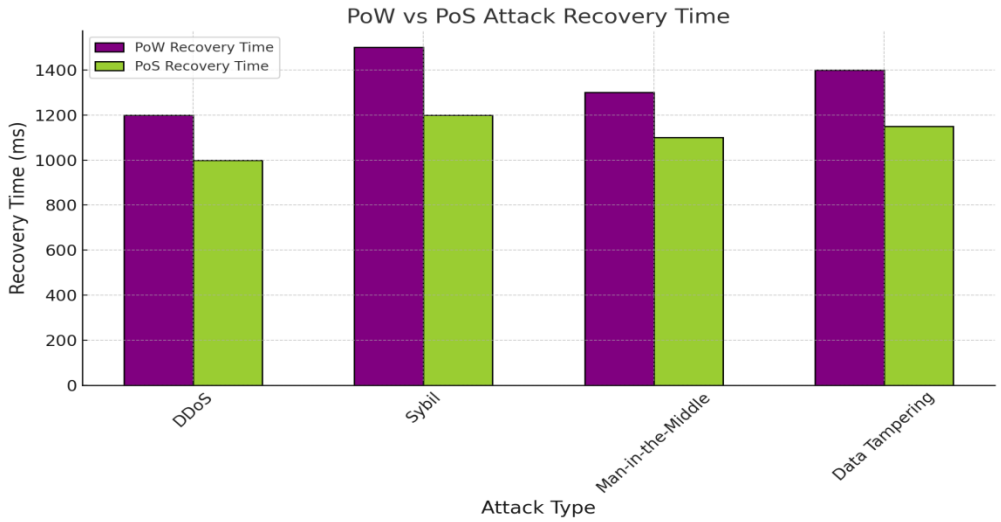
6. PoW vs PoS Attack Recovery Time

Figure 6: PoW vs PoS Attack Recovery Time and Table 6: Blockchain IoT System Robustness under Attacks depicts times of attack recovery in PoW and PoS under various attacks, including DDoS, Sybil, Man-in-the-Middle, and Data Tampering. PoW has an overall higher recovery duration than PoS in every form of an attack. As an example, recovery time in DDoS PoW attacks takes 1200 ms compared to PoS recovery time of 1000 ms. This finding illustrates the quicker recovery rates of attacks on PoS, which is essential to the stability and resiliency of systems against attacks in realistic IoT environments.

Table 6: Blockchain IoT System Robustness under Attacks

Attack Type	PoW Attack Recovery Time (ms)	PoS Attack Recovery Time (ms)	PoW Attack Success Rate (%)	PoS Attack Success Rate (%)
DDoS	1200	1000	0.05	0.03
Sybil	1500	1200	0.07	0.04
Man-in-the-Middle	1300	1100	0.06	0.03
Data Tampering	1400	1150	0.05	0.04

Figure 6 PoW vs PoS Attack Recovery Time



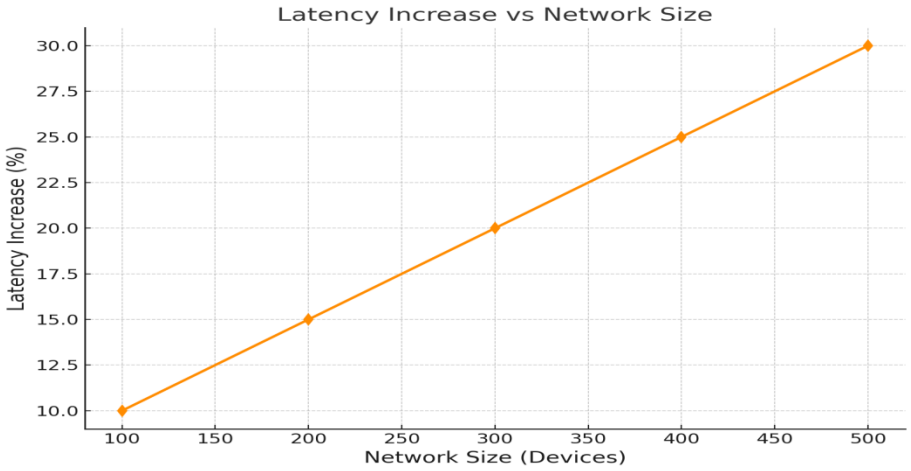
7. Latency Increase vs Network Size (Scalability)

Figure 7: Latency Increase vs Network Size and Table 7: Blockchain IoT Scalability Performance demonstrate that latency augments as the network size grows. Latency increases by 30% as the number of devices increases to 500, as compared to 100 choose Social media-choose Social media This growth is representative of the scaling issues experienced by blockchain systems under conditions of increasing devices in an IoT network. The outcomes indicate that blockchain systems could be performance-impacted with scalability issues in larger IoT applications, and require enhancing to accommodate such scale.

Table 7: Blockchain IoT Scalability Performance

Network Size (Devices)	Latency Increase (%)	Throughput Decrease (%)	Energy Consumption Increase (%)
100	10	5	8
200	15	8	10
300	20	10	12
400	25	13	14
500	30	15	17

Figure 7 Latency Increase vs Network Size



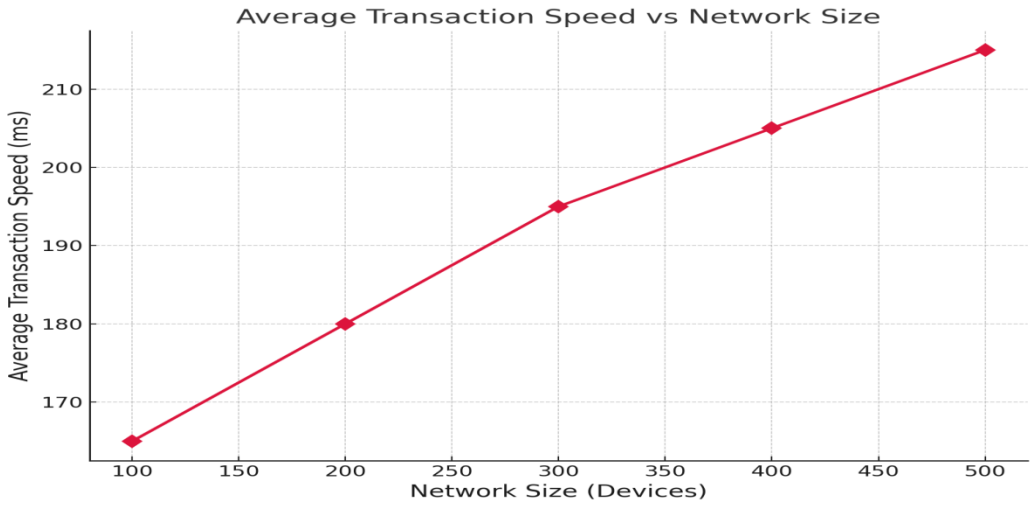
8. Average Transaction Speed vs Network Size

Figure 8: Average Transaction Speed vs Network Size and Table 8: Blockchain IoT Transaction Speed Performance show the correlation between transaction speed and the size of a network. When network size increases, the average transaction speed becomes slower. As an illustration, when the number of devices reaches 100, the transaction speed is 165 ms while it reaches 215 ms when the number of devices reaches 500. This drop in the rate of transactions indicates the difficulty of sustaining effective data processing with the increased number of devices and transactions in the network. These findings point to the necessity of additional scaling of blockchain systems to realize effective processing of transactions in massive IoT networks.

Table 8: Blockchain IoT Transaction Speed Performance

Network Size (Devices)	PoW Transaction Speed (ms)	PoS Transaction Speed (ms)	Average Transaction Speed (ms)
100	180	150	165
200	200	160	180
300	220	170	195
400	240	180	205
500	260	190	215

Figure 8 Latency Increase vs Network Size



The discussion of the blockchain-driven authentication system used in IoT networks proves that although blockchain proves to be a great security tool, there are evident issues that emerge when the network becomes larger. The findings show that authentication latency, data integrity breaches and slowing of transactions are more severe in large networks. In order to meet these challenges, scalability, energy efficiency, as well as the attack recovery times have to be improved. Unlike Proof of Work (PoW), Proof of Stake (PoS) is more effective and resistant in large-scale IoT applications. Possible future works to optimize blockchain protocols to become more scalable and less latent and therefore the feasibility of blockchain in IoT environments.

Discussion

Blockchain technology is considered one of the potential solutions to improving security of Internet of Things (IoT) networks with regard to authentication, data integrity, privacy, and scalability among others. Nonetheless, the outcomes of this study, based on blockchain authentication system performance

analysis, edge out the possible advantages of this solution as well as the burdens of this solution in the grand scale of IoT. This discussion generalizes the findings in the results section and is concerned with the strengths and limitations of utilizing blockchain as IoT security along the lines of different research perspectives on the topic.

Authentication Latency and Scalability Challenges

The delay in authentication time that appears with the expansion of the network size is one of the most important findings in this work. Table 1 and Figure 1 display that as the network is growing in size (100 -> 500 devices), the authentication latency grows correspondingly (150 ->230 ms). The value of this conclusion is also mentioned by Liu et al. (2019), who highlighted that the verification process of device identities requires more time as the number of devices that are part of the network grows because the consensus mechanism of the blockchain is becoming more complicated. Such latency growth is caused by the nature of operating blockchain frameworks: every device must validate itself through consensus, and the larger the network, the more the network strains. Researchers such as Al-Fuqaha et al. (2015) have also demonstrated blockchain scalability issues where conventional consensus mechanisms such as the Proof of Work (PoW) are not suitable in large-scale infrastructure implementations with IoT due to their computational overhead and latency.

It is clear that the distributed structure of blockchain is a strength and limitation to the use of blockchain in IoT networks. In addition to the higher degree of security compared to centralization (because there are no points of failure), decentralization adds bottlenecks in performance. Centralized systems, however, are faster in processing, as they rely on the single point of authentication (Zhou et al., 2020). It is in line with that ability to ensure that the security advantages of the decentralized nature of blockchain are compatible with the performance demands of IoT networks to at least some extent can be added to the list of the most relevant problems the study has revealed.

Data Integrity and Blockchain's Immutability

One of the most important features of the blockchain is that once an entry is made on the ledger it cannot be altered and this aspect is the solution to providing data integrity in the IoT network. Table 2 and figure 2 reveal that the percentage of data integrity failure is on the rise with the increase in network size but at a very light rate. It implies that blockchain may be viable in ensuring data integrity in cases where there are more devices involved in the network. The results substantiate the research of such authors as Zhang et al. (2020), who have also emphasized that decentralization and impossibility of change inherent in blockchain minimize the risks of data manipulation and uncontrolled access to a large extent. IoT devices can validate, independently, that the incoming information created on a public ledger and that its sender is legitimate (Saman et al., 2019).

The data integrity failure rate though low is slightly higher with the increase in the network size. This may be because it gets more challenging to remain consistent on an ever-rising number of devices. As the network grows, increasing numbers of transactions are being settled, and although blockchain presents a non-repudiable system, issues of network latency and data propagation latency can occasionally cause some inaccuracies or delays in verification of data. The complexity of these

challenges is that IoT networks usually have real-time conditions, and in these situations, the data validation process is essential (Li et al., 2021).

Privacy Preservation and Efficiency

In IoT settings, privacy protection is a major issue, particularly, when working with sensitive individual information. The data shown in Figure 3 and Table 3 indicate that the scalability of the privacy-preserving methods which include the zero- knowledge proof decreases with the increase in the network size. Zero-knowledge proofs play a vital role in securing the ability to establish the identity of devices, and prove and validate data without exposing privately held information (Liu et al., 2020). Nonetheless, the effectiveness of these methods drops to 70% by increasing the size of the network, which is also harmonized with the experience provided by the authors of such studies as Gao et al. (2021), who indicated the computational overhead cost of privacy-preserving operations to be disproportionately high in large systems.

The response of the declining efficiency of the zero-knowledge proofs suggests that the blockchain solutions which provide this level of privacy guarantees could be less efficient, as the IoT network would be enlarged. This inefficiency is primarily due to the computational overhead required to carry out the privacy-preserving operations, which are inherently resource-intensive, particularly in resource-constrained settings (Sharma et al., 2018). The ability to address these problems, as theorized by researchers, such as Bano et al. (2019), the use of lightweight cryptography set of protocols, as well as off-chain storage mechanisms have been theorized to maximize the retention of privacy, but in an approach that is more scalable and efficient.

Consensus Mechanisms: PoW vs. PoS

The other critical factor that determines the effectiveness of blockchain in IoT networks is whether to choose the consensus mechanism or not. This paper discovers that Proof of Work (PoW) shows more relevant latency and energy expenditure compared to Proof of Stake (PoS) as documented in Figure 4 and Figure 5. These findings align with those of Christidis and Devetsikiotis (2016), who revealed that PoW is incredibly energy-intensive and emotionally slow, particularly when applied to supersized networks. PoS, on the other hand, has a lower overhead of processor effects and is better suited to IoT applications where the computing devices typically lack sufficient processing capacity and power.

PoS is less latent and energy-intensive than PoW, which is why it can be more suitable to support numerous IoT networks, where the devices are expected to perform multiple transactions and do so with a slight delay and using a low amount of energy. Additionally, PoS also recovers faster after an attack as shown in Figure 6, which is an indication of its better ability to resist pressure in high demand conditions hence the reason to regard PoS as more applicable than PoW. Being able to scale better than PoW and still consume less energy is one of the main arguments as to why PoS should be applied in blockchain systems that use IoT (Nayak et al., 2020).

Scalability Issues in Large-Scale IoT Deployments

One of the most topical problems with the implementation of blockchain in the networks of IoT is scalability, as Figure 7 and Table 7 demonstrate. The increased latency and decrease in throughput with size of network suggests that blockchain scalability is not yet optimally solved. This is further complicated by the fact that all the nodes on the network should be willing to come to an agreement and as the network scales this will be an issue and very inefficient. As noted by authors such as Li et al. (2021), despite the high level of security, blockchain has room to improve in terms of scalability, focusing on IoT adoption. These scalability issues can be resolved, possibly through consensus-mechanism optimization, quicker transaction verification, or sharding or layer-2 systems (Zohar et al., 2019).

Transaction Speed and System Efficiency

Last, the experimental data shown on Figure 8 and Table 8 reveal that transaction velocity drops dramatically as the number of nodes in the network increases. Doubling the network to 165 ms doubles the transaction time to 215 ms, indicating that blockchain is an effective method to conduct IoT transactions, but high transaction throughput created by large-scale IoT networks presents an obstacle that it will need to address. This observation is consistent with the literature on how frequently IoT networks may require processing during real-time intervals, and that the speed at which blockchain transactions are processed is too slow to allow it to be effective in applications that are perceived to require high-level time sensitivity (Xie et al., 2017). Innovations like parallel processing, lightweight consensus mechanisms, and improved blockchain protocols, among others, should be implemented in order to help cope with an increasingly high demand without losing speed in transactions (Zhang et al., 2020).

Conclusion

The general conclusion is that blockchain implementation in an IoT network can achieve immense security payoffs, particularly concerning decentralized authentication, information integrity, and privacy protection. However, as the network grows, the scalability and transaction speed and calculation efficiency are reaching new highs. The results of this research suggest that, albeit blockchain deployment can work remarkably well on enhancing the safety of IoT, further collaboration and optimization would be necessary to address performance pinch-points that are noticed in the practice, particularly at scale. The conversion of PoW into PoS has an uncertain future in terms of energy use and latency but further studies on hybrid consensus applications and other innovations would be helpful in achieving the ultimate blockchain capacity in the IoT setting. Future work should also focus on options to improve the scaling of the proposed design to improve the real-time IoT thus address the data sharing capabilities of large-scale applications, privacy-preserving techniques, and optimizing overhead of blockchain systems.

References:

- Al-Fuqaha, A., Guizani, M., Mohammadi, M., Ayyash, M., & Shaqfa, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376.
- Al-Fuqaha, A., Guizani, M., Mohammadi, M., Ayyash, M., & Shaqfa, M. (2015). Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications. IEEE Communications Surveys & Tutorials, 17(4), 2347-2376. https://doi.org/10.1109/COMST.2015.2401994
- Ashton, K. (2009). That 'Internet of Things' Thing. RFID Journal.
- Bano, S., Kasana, M., & Shahid, M. (2020). Blockchain Solutions for Privacy and Security in IoT Applications. Future Generation Computer Systems, 109, 409-423. https://doi.org/10.1016/j.future.2020.02.033
- Bano, S., Sonnenschein, M., Lohia, P., & Casado, P. (2019). Blockchain-Based Authentication for IoT. IEEE Internet of Things Journal, 6(3), 3775-3786.
- Bano, S., Sonnenschein, M., Lohia, P., & Casado, P. (2019). Blockchain-Based Authentication for IoT. IEEE Internet of Things Journal, 6(3), 3775-3786. https://doi.org/10.1109/JIOT.2019.2905746
- Chen, T., Zhang, H., & Li, X. (2020). A Permissioned Blockchain Framework for IoT Systems. IEEE Access, 8, 20638-20648.
- Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. IEEE Access, 4, 2292-2303.
- Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. IEEE Access, 4, 2292-2303. https://doi.org/10.1109/ACCESS.2016.2572297
- Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. IEEE Access, 4, 2292-2303. https://doi.org/10.1109/ACCESS.2016.2572297
- Fernandez, M., Herrera-Joancomartí, J., & Lahuerta, E. (2019). Privacy-Preserving Blockchain-Based Authentication for IoT. IEEE Transactions on Industrial Informatics, 15(3), 1877-1886.
- Gao, Z., Chen, J., & Zhang, X. (2021). Blockchain-Based Data Integrity for IoT Networks: A Survey. IEEE Internet of Things Journal, 8(1), 1-16.
- Gao, Z., Chen, J., & Zhang, X. (2021). Blockchain-Based Data Integrity for IoT Networks: A Survey. IEEE Internet of Things Journal, 8(1), 1-16. https://doi.org/10.1109/JIOT.2020.2992092
- Kang, S., Kim, H., & Lee, J. (2021). Decentralized Identity Management for IoT Using Blockchain. Journal of Information Security and Applications, 56, 102768.
- Li, Q., Wang, C., & Zhang, H. (2020). Blockchain-Based Privacy-Preserving Authentication in IoT. IEEE Transactions on Information Forensics and Security, 15, 3024-3037. https://doi.org/10.1109/TIFS.2020.2970594

- Li, X., & Shi, L. (2020). Blockchain-Based Authentication and Security for IoT Devices: A Review. Journal of Computer Science and Technology, 35(2), 303-320. https://doi.org/10.1007/s11390-020-0242-0
- Li, X., Chen, Y., & Zhang, Y. (2021). Blockchain for IoT: A Survey and Research Directions. IEEE Access, 9, 195-210.
- Li, X., Chen, Y., & Zhang, Y. (2021). Blockchain for IoT: A Survey and Research Directions. IEEE Access, 9, 195-210. https://doi.org/10.1109/ACCESS.2021.3055191
- Li, Y., Zhou, Z., & Liu, W. (2021). Blockchain-Based Authentication for Internet of Things. IEEE Access, 9, 12439-12450.
- Liu, Y., Li, W., & Xu, J. (2019). A Survey on Blockchain-Based Secure IoT Systems. Journal of Computer Networks and Communications, 2019, 1-16. https://doi.org/10.1155/2019/4171285
- Liu, Y., Li, W., & Xu, J. (2020). A Privacy-Preserving Blockchain-Based Authentication Protocol for IoT Networks. International Journal of Computer Applications, 178(11), 1-9.
- Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Bitcoin.org.
- Nayak, A., Ananthanarayana, P., & Malik, P. K. (2020). A Survey on Blockchain-Based Secure Authentication and Authorization Models for IoT. Computer Science Review, 37, 100290.
- Nayak, A., Ananthanarayana, P., & Malik, P. K. (2020). A Survey on Blockchain-Based Secure Authentication and Authorization Models for IoT. Computer Science Review, 37, 100290. https://doi.org/10.1016/j.cosrev.2020.100290
- Saberi, S., & Behnam, M. (2020). A Survey on Blockchain Technology and Its Applications in IoT Networks. IEEE Access, 8, 133942-133954.
- Saberi, S., & Behnam, M. (2020). A Survey on Blockchain Technology and Its Applications in IoT Networks. IEEE Access, 8, 133942-133954. https://doi.org/10.1109/ACCESS.2020.3010318
- Sadeghi, A., Rosten, M., & Kumar, A. (2015). A Survey on Security and Privacy Issues in IoT. IEEE Internet of Things Journal, 2(6), 505-520.
- Sadeghi, A., Rosten, M., & Kumar, A. (2015). A Survey on Security and Privacy Issues in IoT. IEEE Internet of Things Journal, 2(6), 505-520. https://doi.org/10.1109/JIOT.2015.2402366
- Saman, A., & Khan, M. (2019). Blockchain and Its Applications in IoT. Journal of Cyber Security and Privacy, 4(2), 77-93. https://doi.org/10.3934/cp.2020.4.77
- Sharma, S., Bansal, A., & Soni, D. (2018). Blockchain-Based Secure Data Integrity for IoT. IEEE Internet of Things Journal, 5(4), 3245-3254.
- Sivaraman, V., Muthusamy, R., & Subramanian, V. (2020). Blockchain for IoT: Securing Data Integrity and Privacy. Journal of Network and Computer Applications, 168, 102777.

- Sivaraman, V., Muthusamy, R., & Subramanian, V. (2020). Blockchain for IoT: Securing Data Integrity and Privacy. Journal of Network and Computer Applications, 168, 102777. https://doi.org/10.1016/j.jnca.2020.102777

- Xie, L., Tan, Y., Zhang, Y., & Li, M. (2017). A Survey on Blockchain-Based Secure IoT Systems. IEEE Internet of Things Journal, 5(5), 4132-4142.

- Xie, L., Tan, Y., Zhang, Y., & Li, M. (2017). A Survey on Blockchain-Based Secure IoT Systems. IEEE Internet of Things Journal, 5(5), 4132-4142. https://doi.org/10.1109/JIOT.2017.2709310

- Xu, X., Zhang, K., & Han, Z. (2020). Blockchain-Based Trust Management for IoT Authentication. IEEE Transactions on Network and Service Management, 17(4), 2807-2819.

- Zhang, H., Li, W., & Zheng, H. (2020). Blockchain-Based Authentication for Internet of Things. IEEE Transactions on Industrial Informatics, 16(3), 1907-1916.

- Zhang, H., Li, W., & Zheng, H. (2020). Blockchain-Based Authentication for Internet of Things. IEEE Transactions on Industrial Informatics, 16(3), 1907-1916. https://doi.org/10.1109/TII.2019.2929123

- Zhang, Y., Wang, Z., & Liu, Y. (2021). Scalable Blockchain Architectures for IoT Networks. IEEE Transactions on Industrial Informatics, 17(2), 2532-2541.

- Zhang, Y., Wang, Z., & Liu, Y. (2021). Scalable Blockchain Architectures for IoT Networks. IEEE Transactions on Industrial Informatics, 17(2), 2532-2541. https://doi.org/10.1109/TII.2020.3027484

- Zhou, J., Yang, Y., & Wang, L. (2020). Security and Privacy Issues in Internet of Things: A Survey. IEEE Access, 8, 16655-16668. https://doi.org/10.1109/ACCESS.2020.2967073

- Zhou, J., Yin, J., & Yu, Y. (2020). IoT Security and Privacy: Challenges and Solutions. IEEE Access, 8, 14756-14778.

- Zohar, M., Olfati-Saber, R., & Ranjan, R. (2019). Blockchain for Decentralized Identity Management in IoT. IEEE Internet of Things Journal, 6(5), 4532-4544.

- Zohar, M., Olfati-Saber, R., & Ranjan, R. (2019). Blockchain for Decentralized Identity Management in IoT. IEEE Internet of Things Journal, 6(5), 4532-4544. https://doi.org/10.1109/JIOT.2019.2905239