Journal of Data Acquisition and Processing
ISSN: 1004-9037
https://sjcjycl.cn/
DOI: 10.5281/zenodo.777924

# ANALYSIS OF BLOCKCHAIN INTEGRATION FOR BOLSTERING INTERNET OF THINGS (IOT) COMMUNICATION SECURITY

**Phani Babu Diyyana**
Research Scholar, Shri Venkateshwara University, Gajraula, UP (India)
Email: phanibabu.diyyana@gmail.com

**Dr. Sanjeev Kumar**
Assistant Professor, Maharaja Agrasen Institute of Technology, Guru Gobind Singh Indraprastha University, Delhi

**Dr. Ajay Sharma**
Associate Professor, Kasturi Ram College of Higher Education, Guru Gobind Singh Indraprastha University, Delhi.

**Dr. Deepak Dagar**
Assistant Professor, Maharaja Agrasen Institute of Management Studies, Guru Gobind Singh Indraprastha University, Delhi.

**Anish Soni***
Assistant Professor in Computer Science, Akal Degree College, Mastuana Sahib, Sangrur (Punjab), INDIA, Email: soni_anish@yahoo.com

**Anil Kumar**
Assistant Professor in Computer Science, Public College, Samana, Patiala (Punjab), INDIA
* Corresponding Author

**Abstract -** In recent years, the concept of blockchain technology has garnered substantial attention owing to its pivotal role as the underlying innovation powering cryptocurrencies such as Bitcoin. This surge in interest is particularly notable due to the manifold applications of blockchain technology across diverse domains, including but not limited to, bolstering the security landscape of the Internet of Things (IoT), fortifying the banking sector, optimizing industrial operations, and enhancing clinical establishments. Furthermore, the IoT paradigm has witnessed exponential growth in its adoption, primarily attributed to its seamless integration within smart homes and urban infrastructure projects on a global scale. However, a notable drawback within IoT lies in the inherent limitations of processing power, constrained data storage capacities, and limited network bandwidth of IoT devices. Because of these limitations, IoT devices stand more vulnerable to various forms of cyberattacks in comparison to their counterparts such as smartphones, tablets, or personal computers. This scholarly paper critically delves into the profound security challenges prevalent within the IoT ecosystem and meticulously examines the intricacies of addressing these challenges through the integration of blockchain technology. Additionally, this study identifies and elucidates certain dimensions

that remain inadequately covered by existing blockchain implementations in IoT security contexts. Through this comprehensive exploration, the research aims to contribute to a deeper understanding of the potential and limitations of blockchain in fortifying IoT security, shedding light on unexplored avenues and underscoring the imperatives for future research and technological enhancements.
**Keywords—** IoT security, Blockchain, IoT, Network security, Data security

## 1. INTRODUCTION

The contemporary landscape of the Internet of Things (IoT) is comprised of an assemblage of devices that generate, process, and exchange an extensive array of sensitive data, encompassing both security-critical information and privacy-sensitive content. Consequently, these IoT devices stand as prime targets for a diverse array of cyber threats and attacks [1]. A considerable subset of these newly networkable devices within the IoT realm is characterized by their low-energy profiles and constrained computational capabilities. These devices are mandated to allocate the bulk of their available resources towards executing core application functionalities, rendering the task of concurrently ensuring robust security and privacy a formidable challenge. Traditional security mechanisms, while efficacious, tend to exact a high energy cost and impose significant processing overhead, rendering them less pragmatic for IoT environments [2]. Moreover, several advanced security approaches exhibit pronounced centralization, making them ill-suited for IoT deployments due to scalability issues, the complex many-to-one nature of traffic patterns, and the associated vulnerability to single points of failure [2].

Preserving user privacy within the IoT framework frequently necessitates a trade-off between exposing excessive noise-laden data or furnishing inadequately informative data, which, in turn, can impede the potential for tailored services within IoT applications [3]. Consequently, there exists a pressing requirement for a security and privacy paradigm that is agile, scalable, and possesses inherent distribution. The Blockchain (BC) technology, the foundational backbone of Bitcoin and the inaugural cryptocurrency system, emerges as a potent contender for surmounting the challenges, attributed to its decentralized, secure, and inherently private attributes [4].

In response to escalating security concerns, a pioneering advancement has been introduced in the form of blockchain-secret enhancement. This innovation aims to counteract security vulnerabilities such as unauthorized access to personal data through the mechanism of block requests. The proposal outlines the deployment of intelligent solutions to combat fabricated smart meter data and infringements of personal information.

This comprehensive review paper is organized as follows: Section 1 offers an Introduction to the Intersection of IoT and Blockchain. Subsequently, Section 2 delves into the multifaceted Role of Blockchain within the IoT context, while Section 3 undertakes a meticulous Literature Survey. Expanding on this foundation, Section 4 expounds upon the salient Blockchain Properties. Moving forward, Section 5 elucidates the Security Imperatives specific to IoT. The synthesis of these considerations culminates in Section 6, which outlines the proposition of Enhancing Security and Privacy in the IoT Realm through the Integration of Blockchain. Furthermore, Section 7 navigates through the Spectrum of Blockchain-Based Solutions tailored

for IoT security. In recognition of the complex landscape, Section 8 meticulously dissects the Current Challenges and Intrinsic Issues that converge upon the confluence of Blockchain and IoT (BIoT) Applications. Finally, Section 9 draws the threads together to furnish a comprehensive Conclusion encapsulating the insights gleaned from this scholarly exposition.

### 1.1 Blockchain

The genesis of the Blockchain technology emerges from the realm of Distributed Ledger Technology (DLT). This innovation has been ingeniously designed to introduce a paradigm of protocol validation technology that spans across organizational boundaries, transcending geographical constraints to facilitate seamless and collaborative transactions, inclusive of the entire global landscape. The essence of this instrument resides in its adept ability to circumvent the involvement of intermediary entities, often epitomized by banks, intermediaries, agents, or any intermediaries necessitated to vouchsafe and oversee the validation or alteration of transactional data. This mechanism fundamentally mitigates the necessity for such intermediaries, ushering in a new era of direct peer-to-peer transactions.

The operational architecture of this innovation orchestrates a meticulous sequence of events. Upon the initiation of a financial transaction, the mechanism authenticates the transaction's validity and subsequently encapsulates it within a discrete block, essentially absolving the transaction from any external intervention. Once inscribed within the blockchain, a transaction assumes an immutable state, impervious to manipulation, overwriting, or erasure. This innate quality necessitates a formidable level of security to uphold the sanctity of the transactional record, concurrently ensuring a streamlined and user-friendly experience.

As depicted in Figure 1, the conceptual foundation of blockchain is synergistically intertwined with the domain of the Internet of Things (IoT), culminating in an integrated application ecosystem that offers a profound potential for users. This symbiotic relationship facilitates the realization of an overarching framework where the distributed and secure attributes of blockchain harmonize with the dynamic and interconnected universe of IoT, ushering in an era of transformative possibilities [5].

#### a) Architecture

The blockchain, a fundamental construct within blockchain networks, is an intricate arrangement of interconnected blocks, each meticulously housing a comprehensive record of transactions transpiring within the blockchain ecosystem. As illustrated in Figure 1, the anatomy of a block comprises two quintessential components: the block header and the block body, which encapsulates the transaction count. The block header encapsulates a myriad of critical metadata that contributes to the block's integrity and cohesiveness. It encompasses several vital constituents:

- Block Version: Denoting the software version and validation protocols, this element underscores the versioning of the block.
- Tree Root Hash: A pivotal cryptographic construct, this hash encapsulates the amalgamated hash values of the transactions and a summary of all other data contained within the block.
- Timestamp: Emanating from the epoch of January 1970, the timestamp captures the current universal time, an indispensable feature of the chronological narrative within the blockchain.

- N-Bits: Employed to calibrate the complexity of transaction verification, N-bits ascertain the requisite number of leading zeros within the block hash to render it compliant with the network's consensus rules.
- Nonce: A dynamic 4-byte numerical entity, the nonce commences at zero and systematically increments with each iteration of transaction hashing, bolstering the intricacy of the hash derivation process.
- Parent Block Hash: Signifying a pivotal link to the antecedent block, this hash value embeds the criticality of chronological succession within the blockchain's architecture.

The block's body contains the transaction counter, encompassing a comprehensive enumeration of all enclosed transactions. The upper limit of transactions within a block is contingent upon the block size, exemplifying the inherent scalability of blockchain networks. Conceived as a public ledger, the blockchain unfurls as a sequence of blocks, accommodating pending transactions within its evolving chronicle. The fabric of blockchain's trust is woven through the integration of public key cryptography and distributed consensus mechanisms, which synergistically uphold the security of user interactions. Central to its conceptual framework are attributes of decentralization, persistence, confidentiality, and auditability, which collectively confer upon blockchain technology a transformative potency. These intrinsic qualities transmute into tangible advantages, culminating in cost efficiency and enhanced operational efficacy [6]. An illustration of blockchain which comprises of a nonstop grouping of squares:

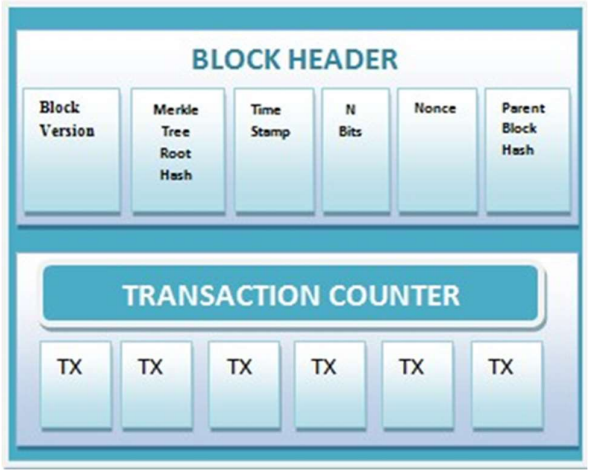


**Fig -1: Block Architecture**

**b) Characteristics**

- Decentralization: In contrast to centralized transaction processing environments, where transactions necessitate validation by a central trusted entity such as a banking system, leading to significant costs and suboptimal performance, the decentralized paradigm of blockchain eliminates the need for intermediaries. Through consensus algorithms, blockchain upholds data integrity and consistency, facilitating a trust less yet secure exchange ecosystem [6].
- Persistency: Upon validation by a mining node—entities validating transactions within a blockchain network—an exchange record is disseminated throughout the entire network. The propagated record becomes immutable and impervious to deletion or

rollback, ensuring the enduring preservation of the transaction's history within the blockchain [6].

- Anonymity: Blockchain leverages public key cryptography to enable nodes' interaction with the network. Through this mechanism, nodes employ public keys to represent their identity, while the actual user identities remain concealed. This cryptographic framework preserves the privacy of network participants [6].
- Security: Security forms the bedrock of blockchain networks, realized through asymmetric cryptographic techniques. These encompass two keys: a public key, employed for addressing within the network, and a private key, used for signing initiated transactions. Transactions are authenticated by validating the transaction creator's identity via their public key [34].
- Robust Backend: Every distributed node within the blockchain IoT network maintains a comprehensive replica of the entire ledger. This architecture not only fortifies the network against potential failures and assaults but also enhances its resilience and robustness [30].
- High Efficiency: The decentralized nature of blockchain obviates third-party involvement, enabling transactions to transpire in low-trust environments. Consequently, the verification time for transactions is significantly reduced, fostering heightened efficiency [34].
- Transparency: Public blockchain networks embrace transparency as a hallmark. All network participants have unfettered visibility into alterations made within the network. Additionally, every transaction is endowed with permanence, rendering them immutable and impervious to alteration [34].
- Smart Contract: A pinnacle achievement within Ethereum, the concept of smart contracts originated from Nick Szabo in 1994. These contracts encapsulate predefined access rights and protocols, programmed into the blockchain. Multiple programming languages, including Solidity, are supported by Ethereum for the purpose of crafting smart contracts, ushering in a realm of automated and tamper-proof interactions [34].

## 2. THE ROLE OF BLOCKCHAIN IN IOT

The Internet of Things (IoT) embodies the transformative capability to facilitate seamless data exchange among diverse physical entities within a heterogeneous network. The IoT landscape delineates several distinct domains, each with its unique functionalities:

- Physical Entities: The IoT introduces distinct identities for every interconnected entity within the network, enabling seamless data exchange among these physical entities.
- Gateways: Functioning as intermediaries, gateways orchestrate the interaction between physical entities and the cloud infrastructure, ensuring the establishment of secure and efficient connections.
- Networking: The networking facet regulates data flow and endeavors to establish the most efficient pathways between IoT nodes, facilitating optimized data exchange.
- Cloud: Serving as a repository and computational hub, the cloud stores and processes voluminous data generated by IoT interactions.

The blockchain technology, a compilation of cryptographically verified and linked transactional blocks, serves as a cornerstone within this IoT milieu. These blocks encapsulate

data and transactions and are stored in a shared, publicly accessible digital ledger. Notably, blockchain furnishes a secure communication framework within the IoT network. Depending on its configuration, a blockchain can manifest as private, public, or a consortium with varying attributes, each tailored to specific requirements. The ensuing differentiation is encapsulated in the subsequent table [10], illustrating the spectrum encompassing different types of blockchains.

**Table I. Types of blockchains**

| Property | Blockchain Types |
|---|---|
| Trust Model | Decentralized in Blockchain, Centralized in Centralized Database |
| Security | High in Blockchain, Low in Centralized Database |
| Accessibility | Highly accessible in Blockchain, Low accessibility in Centralized Database |
| Privacy | Ranges from Low to High in Blockchain, High in Centralized Database |
| Identity Flexibility | Flexible in Blockchain, Non-flexible in Centralized Database |

Distinctly, the database in a blockchain embodies attributes such as a decentralized trust model, elevated security, widespread accessibility, variable privacy levels, and adaptable identities. Conversely, in a centralized database, a centralized trust model prevails, security is compromised, accessibility is limited, privacy is elevated, and identities are less flexible. Consequently, the blockchain's properties significantly surpass those of the centralized storage solution. The integration of IoT with blockchain heralds an era of advanced security, data transparency, and robust communication, poised to transform the dynamics of technological ecosystems.

## 3. LITERATURE SURVEY

The years 2017 and 2018 witnessed a marked surge in the deliberation and exploration of security and privacy concerns within IoT communication, reflected through a multitude of scholarly publications. Notably, the conceptual roots of blockchain technology trace back to a seminal work by Stuart Haber and W. Scott Stornetta in the 1990s, where they elucidated the concept of preserving document privacy without the necessity of storing information in the timestamping service [7]. The foundational framework of blockchains began to crystallize through these ideational contributions; however, the first instantiation of blockchain came forth in 2008 with Satoshi Nakamoto's seminal paper. Nakamoto introduced the concept of blocks linked in a sequential chain, thus paving the way for the creation of the blockchain structure [4].

Among these developments, the inception of the "IoT Chain" emerges as a significant milestone [9]. This work entails the authentication of data exchanged between nodes within an IoT network through the formulation of an algorithm that harmonizes IoT and blockchain. This paper specifically delves into the pivotal realm of authorization within the IoT Chain framework. Furthermore, the scholarly landscape expanded to encompass various other pivotal dimensions. The article authored by [11] delves into the integration of the cloud and Mobile Ad-Hoc Network (MANET) framework to establish secure communication channels for smart IoT devices. [12] presents an innovative paradigm known as the "Internet-Cloud Framework," which remarkably augments secure communication within IoT devices. Complementary to this, [13] introduces a middleware architecture situated within the cloud-MANET ecosystem, fostering seamless data accessibility among IoT devices. In the pursuit of enhanced communication reliability among IoT nodes, articles such as [14, 15] assume prominence.

These works delve into the intricacies of bolstering communication dependability. Amidst the paradigm shift to 5G networks, [10-15] unveil versatile models designed to optimize communication. [21] further propounds a communication security framework grounded in fuzzy logic principles.

A comprehensive survey on the intersection of blockchains and IoT is meticulously crafted within [16]. This work elucidates the intricate security considerations intrinsic to the amalgamation of these two realms. The article contemplates the potential of blockchain technology to empower IoT applications with robust security attributes. In summation, the years under examination have witnessed a prolific discourse on security and privacy aspects within IoT communication, culminating in a diverse array of insights and frameworks that continue to shape the trajectory of secure IoT deployment.

## 4. BLOCKCHAIN PROPERTIES

- Blockchain Working Steps: Nodes engage with the blockchain network through a combination of private and public keys. Users utilize their private keys to digitally sign their transactions and access the network through their public keys. Each signed transaction is then broadcasted by the initiating node [8]. The transaction undergoes verification by all nodes within the blockchain network except the one that initiated the transaction. This validation step, referred to as verification, involves the elimination of invalid transactions. Subsequently, the process of mining ensues. During this phase, legitimate transactions occurring within a specific timeframe are gathered by network nodes into a block. These nodes then conduct a proof-of-work computation to discover a nonce for the block. Upon finding a nonce, the node broadcasts the block to all participating nodes [4]. Each node receives the newly generated block and performs two key verifications: (a) validation of legitimate transactions and (b) affirmation of the parent block's accuracy through hash computation. Upon successful verification, the block is appended to the blockchain, and the transactions are executed to update the blockchain. If a block fails to gain confirmation, it is rejected, thereby concluding the mining cycle [8].
- Verification: Blockchain technology leverages asymmetric cryptography, employing private and public keys, to eradicate issues of duplication. The private key remains confidential to the generating node, while the public key is disseminated across the network. The node initiating the transaction digitally signs it, and the signature is propagated throughout the blockchain network. Receiving nodes validate the transactions by decrypting the signature using the public key of the originating node. The transaction's authenticity is established through signature verification, ensuring that the initiating node's identity remains unaltered [29].
- Proof of Work (PoW): The proof-of-work process entails identifying a value that, when hashed using the Secure Hash Algorithm 256, meets the predetermined difficulty criteria. The extent of computational effort required is adjustable, ranging from zero to the required number of leading zeros in the hashed output. In a decentralized blockchain network, all nodes participate in the proof-of-work for each mining cycle by iteratively altering a nonce value within the block until the desired hash is achieved. Once the computational effort has been expended to satisfy the proof-of-work requirements, the

block becomes immutable, barring any alterations without repeating the entire proof-of-work process. The integration of blockchain and IoT data management facilitates distributed data access, offering users the ability to share data with third-party entities while avoiding centralization, thereby safeguarding user data [4].

## 4. SECURITY REQUIREMENTS FOR IOT

### a) Data Privacy, Confidentiality, and Integrity

The dynamic trajectory of IoT data traversing through various network nodes necessitates a robust encryption mechanism to ensure data privacy. The amalgamation of diverse devices, services, and networks renders the data stored on devices susceptible to privacy breaches, potentially resulting from compromised nodes within the IoT ecosystem. Additionally, IoT devices vulnerable to attacks can enable adversaries to manipulate data integrity, thereby posing a threat to the veracity of stored information.

### b) Validation, Authorization, and Accounting

The establishment of secure communication within IoT mandates the implementation of authentication between communicating parties. For controlled access to services, devices require rigorous authentication. However, the heterogeneous nature of underlying models and environments supporting IoT devices has led to a proliferation of authentication methods. These circumstances present a challenge in devising a standardized global protocol for IoT authentication. Moreover, authorization mechanisms ensure access only to legitimate entities, culminating in a secure environment for communication. Incorporating resource usage tracking, auditing, and reporting mechanisms bolsters network management security [17].

### c) Energy Efficiency

IoT devices are often resource-constrained, characterized by limited power and storage capacities. Breaches in IoT systems may lead to energy consumption surges due to network flooding through spurious service requests. To address this, energy-efficient solutions are imperative, considering IoT endpoints predominantly rely on battery-powered equipment. Paradoxically, some blockchain implementations are energy-intensive, primarily due to mining processes that involve computational power-intensive proof-of-work (PoW) algorithms [19].

## 5. PROVIDING SECURITY AND PRIVACY IN IOT VIA BLOCKCHAIN

IoT devices generate, process, and transmit voluminous data over the Internet, potentially leading to privacy concerns. Blockchain can play a pivotal role in the development of decentralized applications for vast device networks. Determining when and how to apply this technology to ensure security and privacy presents a challenge. Authors have examined the intersection of Blockchain and IoT, addressing issues like:

- Limited capabilities of typical IoT devices.
- Transaction costs affecting interactions.
- Latency in IoT endpoints.
- The need for confidentiality of IoT-generated data.

Hence, exploring the applicability of both technologies is essential. This involves:

- Developing cost-effective Blockchain solutions suitable for low-capacity devices.
- Facilitating micropayments between sensors for data exchange.
- Enabling computation and data extraction from sensitive data.
- Integrating with smart homes, smart cities, and shared economy platforms.

The integration of Blockchain and IoT presents opportunities, but the inherent vulnerabilities of Blockchain must be acknowledged when crafting new applications [20, 15].

### 5.1 Utilization of Blockchain to Provide Anonymity and Access Control to IoT

Preserving privacy poses a formidable challenge in the realm of IoT, given that interconnected "things" accumulate sensitive personal data and unveil the behavioural patterns of their proprietors. A recommendation to address this challenge involves the development of IoT applications utilizing an established and secure Blockchain system [21, 22]. This approach, backed by PoW and a multitude of trustworthy miners, could enhance privacy. It's important to note that the confidentiality afforded by Blockchain is not absolute but rather termed pseudo anonymity. Certain conditions can lead to the deanonymization of transaction owners or their IP addresses. Several specific techniques for deanonymization include:

- Multiple Inputs: In certain instances, resolving a specific transaction requires aggregating balances from various accounts, and in others, consolidating the total wallet balance into a single account. This process, termed multiple inputs transaction, requires access to private keys, implying all accounts belong to the same user.
- Change Address: When conducting a transaction, all associated balances must be accounted for. If the transaction value differs from the balance assigned to the key, a change occurs. This change must return to the owner, effectively linking addresses and revealing the user's transactions.
- IP Association: Bitcoin operates as an overlay network atop the Internet. Network messages are often transmitted in broadcast to nearby nodes. Monitoring network traffic and using clustering algorithms can associate IP addresses with users, as demonstrated by [33].
- Centralized Services: Users may entrust the management of their private keys to third-party services, a practice criticized by some as a privacy risk. These outsourced services may inadvertently expose identities or resources, and in some cases, exploit the funds across all user balances [31, 34].

### 5.2 Blockchain in Economic Scenarios for IoT Transaction Assurance

- The IoT envisions a future characterized by a network of autonomous devices capable of independent communication and decision-making. The incorporation of Blockchain can foster this IoT vision by establishing a foundation to facilitate a machine-to-machine (M2M) communication-based sharing economy.
- Blockchain will underpin transaction processing and coordination among devices, leading to the Internet of Decentralized, Autonomous Things. A prototype implementation of electronic data exchange between a sensor and a consumer through Bitcoin network is outlined. The system consists of three components:
- IoT Device: Responsible for tasks such as generating a data request upon receiving payment and creating and publishing a transaction containing the requested data.
- Client: Facilitates payment to the sensor and monitors Blockchain changes to detect transactions containing data from the IoT device.
- IoT Device Registry: A repository of registered sensors that can be located by clients. Entries include sensor address, offered data, cost, and metadata such as location [28].

## 6. BLOCKCHAIN SOLUTIONS FOR IOT

**a) Data Integrity**

The blockchain functions as a distributed network where all nodes possess identical copies of records. When a transaction is initiated, the initiating node signs it with its private key and shares it with other nodes for validation. Participating miner nodes engage in a verification process, seeking a nonce. The first node to discover the nonce gains the privilege to validate the transaction and receive a reward. The newly formed block is then broadcasted to all nodes in the entire network. Once recorded in the blockchain, data cannot be altered or deleted [30].

**b) Data Privacy**

Consortium blockchains offer data privacy within a blockchain network. Nodes serving a specific purpose are grouped together to establish a private network or side chain. Each side chain autonomously manages its IoT data. Nodes within one side chain cannot participate in the validation process of other side chains. Access to consortium blockchain data requires node registration in the relevant side chain network. This approach ensures controlled access and prevents unauthorized entry [31].

**c) Address Space**

The blockchain encompasses a 160-bit address space in contrast to IPv6's 128 bits. These 160 bits are generated by the Elliptic Curve Digital Signature Algorithm (ECDSA). With 4.3 billion more addresses than IPv6, blockchain offers enhanced address distribution compared to IPv6 [32].

**d) Trusted Accountability**

Every action record is uploaded to the blockchain network, endowing each action with a unique identity and making them traceable. When anomalous behavior is detected within an entity, blockchain can be employed for further investigation [30].

**e) Fault Tolerance**

Decentralized devices are less prone to failure due to their reliance on multiple independent components. Blockchain functions as a point-to-point decentralized network where each device possesses an identical copy of the ledger, rendering the failure of a single node inconsequential to the network. Thus, blockchain eliminates single points of failure [4].

**f) Trusted Data Origin**

A unique identifier is assigned to each IoT device for data tracking within the blockchain network. Data collected from a device is linked to its identifier and, after data hashing, is shared with the entire network. This establishes a trusted data source [30].

**g) Eliminating Third-Party Risks**

Blockchain empowers devices to operate without intermediaries or third parties, reducing third-party risks [4].

**h) Access Control**

Smart contracts can be developed on blockchain to define access rights and policies. For instance, a rule can be established that devices enter energy-saving mode when the meter reaches 135 KW.

**i) Preventing Unauthorized Personal Data use**

Blockchain's Peer-to-Peer (P2P) storage systems can verify and record all actions on IoT network data, prohibiting the illicit use of personal data. Consortium Blockchain for IoTs is proposed as an extension of security at multiple levels [31].

### j) IoT Network Data Sharing

As the scale of IoT network data sharing expands, so does the cost of key storage. Databases are maintained at remote origins, with a centralized server retaining references to these sources. Blockchain is used to manage the Reference Integrity Matrix (RIM) of the database. With blockchain's immutability feature and universal access of RIM through all IoT devices, the integrity of RIM is assured. The integrity of RIM can be confirmed by comparing it with the maintained RIM on the blockchain every time an essential Information Set is extracted from the origin [33].

## 7. CURRENT CHALLENGES AND ISSUE FOR BLOCKCHAIN AND IOT (BIOT) APPLICATIONS

- BIoT endpoints typically benefit from power-based hardware equipped with batteries. Therefore, achieving energy efficiency is crucial for ensuring the sustainability of node deployment over the long term.
- Maintaining confidentiality for an individual user relies on effectively managing their personal keys. Attackers seek to either steal from or impersonate the user through access to their public key. An initiative addressing this concern is CONIKS.
- In the blockchain, all users were identified by their hash or public key. This lack of true anonymity stemmed from the sharing of complete transactions, enabling third parties to analyze and deduce participants' identities.
- BIoT applications might demand a blockchain network capable of processing a large volume of transactions within specified time intervals in clear networks. While consensus latency was influenced more by agreement method intricacies than by excessive hashing.
- Operators storing their transactions necessitated longer initial transaction times while benefiting from the most powerful miners' capabilities.
- Adjustments to transaction and block volume had to be made to align with IoT network bandwidth limits.
- To facilitate designers' work, Blockchain entry through user-friendly Application Programming Interfaces (APIs) would be recommended.
- In many instances, the proliferation of blockchains has led to the need for simultaneous interaction with multiple chains. This could also be the case for BIoT.
- Forking of blockchains can occur for development or governance purposes. Historically, exchanging transactions between two forked blockchains posed challenges.
- Clear legal regulations for promoting smart contracts and dispute resolution are yet to be adequately established. Efforts are underway to reconcile traditional contracts with smart contract technology.

## 9. CONCLUSIONS

This paper aims to provide a comprehensive literature review on the integration of Blockchain technology and the Internet of Things (IoT), addressing the associated challenges in an IoT environment. As IoT gains prominence with rapid network expansion and intelligent device proliferation, security vulnerabilities become a pressing concern. This review highlights the

distinctive attributes of blockchain networks that offer potential solutions to mitigate IoT issues.

The review delves into crucial aspects such as the fundamentals of Blockchain, its core functions, various types of Blockchains, and the interaction between Blockchain and IoT. Extensive research indicates that the amalgamation of these two technologies has the potential to alleviate the prevailing security issues in IoT applications. The integration of Blockchain and Internet of Things presents a promising avenue for enhancing security and privacy in the realm of IoT. This paper underscores the urgent need for robust security mechanisms in the face of the burgeoning IoT landscape. The synthesis of Blockchain and IoT not only offers a novel solution to address security concerns but also introduces transformative capabilities to tackle the intricate security challenges posed by the ever-expanding network of Internet-connected objects. Further research in this direction is crucial to fully harness the synergistic potential of these two innovative technologies.

**REFERENCES**

[1] Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in internet of things: The road ahead. Computer Networks, 76, 146-164.

[2] Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. Computer Networks, 57(10), 2266-2279.

[3] Chakravorty, A., Wlodarczyk, T., & Rong, C. (2013). Privacy preserving data analytics for smart homes. In Security and Privacy Workshops (SPW), 2013 IEEE (pp. 23-27). IEEE.

[4] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

[5] Michael, J., Cohn, A., & Butcher, J. R. (2018). Block Chain technology. The Journal. Retrieved from: https://www.steptoe.com/images/content/1/7/v2/171967/LITFebMar18-Feature-Blockchain.pdf

[6] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. Big Data (Big Data Congress) IEEE International.

[7] Haber, S., & Stornetta, W. S. (1990). How to timestamp a digital document. Conference on the Theory and Application of Cryptography. Springer, Berlin, Heidelberg.

[8] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. IEEE Access, 4, 2292-2303.

[9] Alphand, O., et al. (2022). IoT Chain: A blockchain security architecture for the Internet of Things. Wireless Communications and Networking Conference (WCNC), 2018 IEEE. IEEE.

[10] Alam, T. (2019). Blockchain and its Role in the Internet of Things (IoT). International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 5(1).

[11] Alam, T., & Benaida, M. (2018). The Role of Cloud-MANET Framework in the Internet of Things (IoT). International Journal of Online Engineering (iJOE), 14(12).

[12] Alam, T., & Benaida, M. (2018). CICS: Cloud-Internet Communication Security Framework for the Internet of Smart Devices. International Journal of Interactive Mobile Technologies (iJIM), 12(6).

[13] Alam, T. (2017). Middleware Implementation in CloudMANET Mobility Model for Internet of Smart Devices. International Journal of Computer Science and Network Security, 17(5).
[14] Alam, T. (2018). A Reliable Communication Framework and Its Use in Internet of Things (IoT). International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), 3(5).
[15] Alam, T. (2018). A reliable framework for communication in internet of smart devices using IEEE 802.15.4. ARPN Journal of Engineering and Applied Sciences, 13(10).
[16] Conoscenti, M., Vetro, A., & De Martin, J. C. (2016). Blockchain for the Internet of Things: A systematic literature review. Computer Systems and Applications (AICCSA), 2016 IEEE/ACS 13th International Conference of. IEEE.
[17] Salah, K., & Khan, M. (2022). IoT Security: Review, Blockchain Solutions, and Open Challenges. Future Generation Computer Systems, 82.
[18] Jesus, E. F., Chicarino, V. R. L., Albuquerque, C. V. N. de, & Rocha, A. A. de A. (2018). A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack. Security and Communication Networks, vol. 2018, Article ID 9675050.
[19] Alamri, M., Jhanjhi, N. Z., & Humayun, M. (2019). Blockchain for Internet of Things (IoT) Research Issues Challenges & Future Directions: A Review. IJCSNS International Journal of Computer Science and Network Security, 19(5).
[20] Dorri, A., Kanhere, S. S., & Jurdak, R. (2016). FairAccess: a new Blockchain-based access control framework for the Internet of Things. Security and Communication Networks, 9(18), 5943-5964.
[21] Conoscenti, M., Torino, D., Vetr, A., & De Martin, J. C. (2016). Blockchain for the Internet of Things: a Systematic Literature Review. IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA).
[22] Ouaddah, A., Abou Elkalam, A., & Ait Ouahman, A. (2017). FairAccess: a new Blockchain-based access control framework for the Internet of Things. Security and Communication Networks, 9(18), 5943-5964.
[23] Spagnuolo, M., Maggi, F., & Zanero, S. (2022). Bitiodine: Extracting intelligence from the bitcoin network. International Conference on Financial Cryptography and Data Security, pp. 457–468, Springer.
[24] Moser, M., Bohme, R., & Breuker, D. (2013). An inquiry into money laundering tools in the Bitcoin ecosystem. Proceedings of the 2013 APWG eCrime Researchers Summit, eCRS 2013, IEEE, USA.
[25] Herrera-Joancomartí, J. (2015). Research and Challenges on Bitcoin Anonymity. Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance, vol. 8872, pp. 3-16, Springer.
[26] Koshy, P., Koshy, D., & McDaniel, P. (2014). An analysis of anonymity in bitcoin using P2P network traffic. Proceedings of the International Conference on Financial Cryptography and Data Security, pp. 469-485, Springer.
[27] Valenta, L., & Rowan, B. (2014). Blindcoin: blinded, accountable mixes for Bitcoin. Proceedings of the International Conference on Financial Cryptography and Data Security, pp. 112-126, Springer.

[28] Wörner, D., & Von Bomhard, T. (2022). When your sensor earns money: Exchanging data for cash with Bitcoin. Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing, UbiComp 2014, pp. 295-298, ACM.
[29] Pilkington, M. (2016). Blockchain technology: Principle and applications. Research Handbook on Digital Transformations.
[30] Liang, X., Zhao, J., Shetty, S., & Li, (2017). Towards data assurance and resilience in IoT using blockchain. Conference Paper.
[31] Ali, M. S., Dolui, K., & Antonelli, F. (2017). IoT data privacy via blockchains and IPFS. International Conference on the Internet of Things (ACM, New York).
[32] Antonopoulos, A. M. (2014). Mastering Bitcoin. First Edition. O'Reilly Media, USA.
[33] Banerjee, M., Lee, J., & Choo, K. K. R. (2021). A Blockchain future for internet of things security: a position paper. Digit. Commun. Networks, 4(3), 149-160.
[34] Sultan, A., Mushtaq, M., & Abubakar, M. (2022). IOT Security Issues Via Blockchain: A Review Paper. 60-65. 10.1145/3320154.3320163.