

Blockchain-Enabled IoT: Ensuring Data Integrity in a Connected World

^[1] Ajay Kumar B R, ^[2] Dr Puttegowda D

^[1]Research Scholar, Dept. of CSE, ATME College of Engineering, Mysore
Asst Professor Dept of ISE MITMysore Affiliated to VTU

^[2] Professor and HOD Dept of CSE, ATME College of Engineering, Mysuru Affiliated to VTU

Abstract— Internet of Things (IoT) has connected everyday objects to the internet, creating opportunities for data-driven insights. However, traditional IoT systems using centralized cloud servers often lead to isolated data storage and raise concerns about data security and privacy. To address these issues, the paper introduces a system that combines blockchain technology with IoT sensors. This system focuses on being modular, efficient with data, and available while using lightweight encryption methods suitable for resource-limited IoT devices.

One key concept introduced is "proof-of-authentication," where sensor nodes create authentication tags based on their data. These tags are verified by cluster head nodes before being added to the blockchain. The paper demonstrates that this approach can authenticate data quickly, making it suitable for IoT devices with limited resources.

The paper also highlights the growing importance of blockchain in various sectors, including industry, government, and academia, similar to the early days of cloud computing and IoT. However, challenges remain, particularly in industrial IoT (IIoT). The paper discusses the latest developments in blockchain-enabled IoT applications and outlines future research directions. It emphasizes the need for collaboration with organizations to turn blockchain-based IoT solutions into practical applications.

In summary, this paper contributes to our understanding of integrating blockchain into IoT systems. It provides design principles, management insights, and technological recommendations, exploring how IoT and blockchain can transform industries. It acknowledges the need for ongoing research and collaboration to fully realize their potential.

Index Terms- Centralized cloud servers, industrial IoT (IIoT), Lightweight cryptographic solutions, IoT sensor nodes

1. Introduction

IoT (Internet of Things): Internet of Things connects all the devices to the internet allowing them to communicate with each other over the internet. In India, agriculture is the largest livelihood provider without any question. Since the population rises, there is a need for agricultural products. To support greater production in farms, the requirement of the amount of freshwater used in irrigation also rises. Currently, agriculture accounts for 83% of the total water consumption in India. Hence, wastage of water must be controlled by taking. Internet of Things is a huge network of connected devices – all of which gather and share data about how they are used and the environments in which they are operated. IoT works in different domains of farming to improve time efficiency, water management, crop monitoring, soil management, control of insecticides, pesticides and fertilizers. There are systems which are completely automated and there is no need for human intervention. Also, the sensor readings are transmitted to a Thing speak channel to generate graphs for analysis. It is the application of modern Information and Communication Technologies into agriculture. In IoT-based smart farming, a system is built for monitoring the crop field with the help of sensors (light, humidity, temperature, soil moisture, etc.) and automating the irrigation system.

Blockchain: A block chain technology is a digital ledger of record of transactions, which based on decentralized network (Fig.1) in a peer-to-peer network around the world [2] .Block chain, is focused primarily online transactions and disseminated digital ledger system.

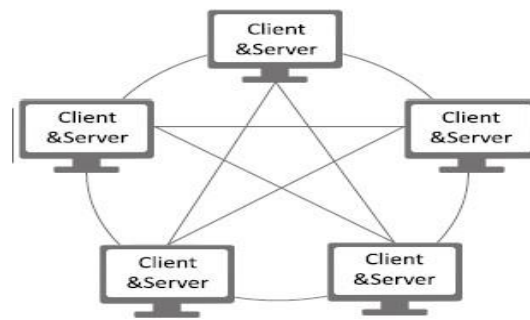


Fig 1. Decentralized network

Block chains consist of blocks or data records and each block is linked to the next block in an irreversible chain [2] and the transactions are gathered as a block –hence the term “block chain”. While comparing with traditional centralized database, the information cannot be handled due to block chain’s feature of distributed nature and confirmed guarantees by the peers. If someone wants to perform a transaction, it goes to the network directly and algorithms find the authenticity of the transaction. After the transaction is verified, the new one is linked with the previous transaction forming a chain of transactions. This chain is called the block chain. The agreement between two people in the form of a computer code is called as Smart Contract. They run on the block chain, so they are stored on a public database Proceedings and cannot be changed [2]. The combination of block chain technology and smart contract gives more flexibility to design, develop and implement in real-time with minimum cost. Block chain-based smart contracts provide number of advantages: they are quick and real-time refurbish, minimum cost and lower risk in execution, no intermediaries and high accuracy. More sensitive business areas such as supply chain [2], IoT (Internet of Things) [2] and banking [2] are deployed as permissioned smart contracts [2]

2. Related Works:

In the field of blockchain and IoT, several surveys have been conducted, and they can be categorized into three main groups. Let's briefly discuss these surveys and highlight the limitations of the existing state-of-the-art reviews.

The first category of surveys primarily explores the technical aspects and broader applications of blockchain technology. For instance, in [5], Li et al. conducted a comprehensive review of security attacks and vulnerabilities in blockchain systems. Casino et al. [6] reviewed blockchain applications across various domains, including business, education, finance, and IoT. In the same year, Wu et al. [7] examined both the theoretical foundations of blockchain and its practical application in IoT.

The second category of surveys delves into IoT, focusing on its architecture, applications, and security aspects. In [8], Viriyasitavat et al. reviewed the application of blockchain for IoT from a system design perspective.

Distinct from the previous categories, the third group of surveys evaluates the application of blockchain to enhance IoT systems. In [9], Fernandezcarames and Fragalamas reviewed optimized blockchain solutions for IoT, considering aspects such as architecture, cryptographic algorithms, message timestamping, and consensus mechanisms. In [10], Lo et al. provided insights into blockchain-enabled IoT applications from the perspectives of data management and device management.

Despite these valuable surveys, there are limitations in the existing state-of-the-art reviews. The first two categories tend to focus solely on either blockchain or IoT, lacking a comprehensive examination of their interaction. In contrast, the third category examines the synergy between blockchain and IoT but often has a narrow focus, either concentrating on specific applications or in-depth analysis of optimized blockchain technologies. Our review offers a novel perspective by emphasizing the unique functionalities of blockchain that can enhance existing IoT applications. Additionally, we present a comparison with recent state-of-the-art reviews in paper. Furthermore, in Section 7, we consolidate general strategies for leveraging blockchain to create

dependable IoT applications, which we believe can be valuable for researchers and developers looking to integrate blockchain into their IoT projects.

In contrast, our review seeks to bridge these gaps by offering a fresh perspective. We emphasize the distinctive capabilities of blockchain that can augment and fortify existing IoT applications. Furthermore, we provide a comparative analysis with recent state-of-the-art reviews, offering researchers and developers a holistic view of the evolving landscape. In Section 7, we distill general strategies for effectively integrating blockchain to enhance the reliability and security of IoT applications. These insights aim to empower those seeking to leverage blockchain's potential within their IoT projects, addressing the limitations observed in prior surveys.

3. Methodology And System Architecture:

IoT system architecture:

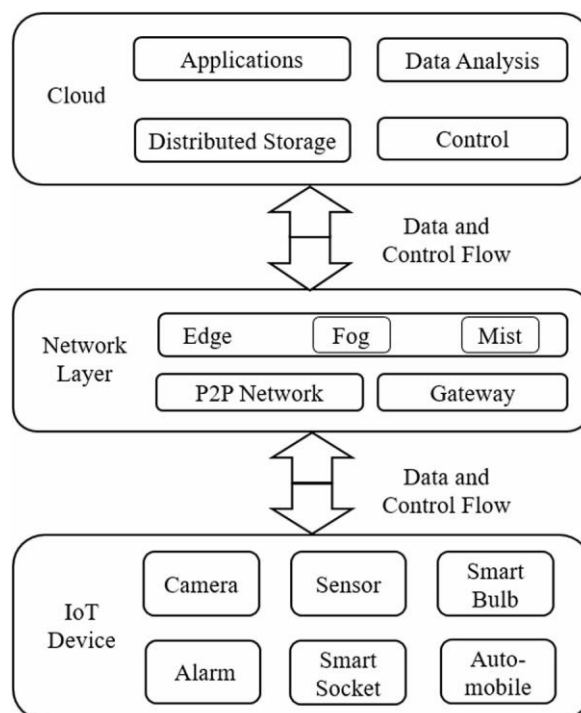


Fig 2. Typical IoT system architecture.

The architecture of the Internet of Things (IoT) is a sophisticated framework designed to facilitate the seamless interconnection of myriad physical devices and sensors with the digital world. At its core are the IoT devices and sensors scattered across homes, industries, and cities, collecting data from the environment. These devices communicate through diverse connectivity options, including Wi-Fi, cellular networks, and low-power protocols, and they often incorporate edge computing capabilities to process data locally for quicker responses. A crucial component in IoT architecture is the gateway, which aggregates data from multiple devices before forwarding it to the cloud. In the cloud, data is stored, analyzed, and visualized on scalable platforms, enabling real-time insights and historical trend analysis. IoT applications and services are built on top of this data, empowering users to control connected devices and harness the information for improved decision-making. Security plays a paramount role, with encryption, authentication, and access control measures to safeguard IoT ecosystems from potential threats. The user interface, typically in the form of mobile apps or web dashboards, offers end-users the ability to monitor and interact with IoT devices, making it accessible and user-friendly. Scalability, device management, and adherence to regulatory standards are additional considerations, ensuring that IoT systems can grow and adapt while maintaining data privacy and compliance. In essence, the IoT architecture creates an interconnected web of smart devices, offering automation, efficiency, and valuable insights across various domains, from smart homes to industrial automation and beyond.

4. Blockchain system architecture:

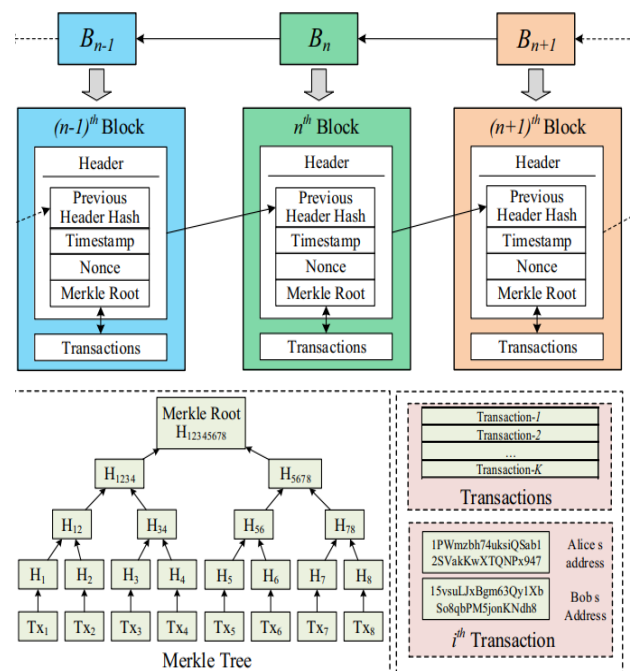


Fig.3 Blockchain system architecture.

In a typical blockchain system such as Bitcoin or Ethereum, miners add valid transactions to a block, and a Merkle Root [4] is created for all these transactions as a digest or fingerprint [4]. As shown in the Fig. 2, a block header contains the hash of the previous block header, timestamp, a nonce, and the Merkle root of the transactions in the current block. All the blocks are connected in the form of a linked list, which is a type of data structure in which each data element contains a link to its successor or predecessor. As the whole network works on the same single chain, for a certain period of time, only a limited number of transactions can be validated by the newly generated block [4]. Thus, the block generation interval and the block size determine the transaction verification speed. For example, Bitcoin can append a new block with block size 1 MB every 10 min, which yields 3–7 transactions verified per second [4]. Instead of packing a group of transactions into a block and forming a chain in a linked list, another blockchain structure has been proposed that is based on the concept of directed acyclic graph (DAG). In the model of DAG blockchain, there is no need to encapsulate transactions into a block, and each transaction may represent a data point in the DAG. A notable DAG-based blockchain structure is Tangle, which was designed by IOTA [4]. In Tangle, one needs to verify two previous transactions and link the new transaction with the previous two to append a new transaction. An example of two types of blockchain structure is shown in Fig. 3. In the linked list blockchain, a certain number of transactions can be appended to the blockchain in a time interval. However, in a high transaction rate scenario, not all the transactions can be added, as with the transactions with red Tx tags in Fig. 3a. On the other hand, transactions and blocks can be appended to the blockchain in a flexible and efficient manner by using a DAG based structure. As shown in Fig. 3, the transactions with red Tx tags can also be added to the chain.

Blockchain Applications in IoT

From a IoT perspective, blockchain is a promising technology that can offer multidimensional reinforcements for the IoT infrastructure. As mentioned in PAPER, blockchain can contribute to the following aspects:

- **Service management:** As we know, the native and fundamental component of blockchain is the transaction, and the transaction-based blockchain architecture can help with the IoT service payment, which also enables IoT objects to perform real-time, automatic, and microtransactions in a M2M manner. The concept and a case study of the blockchain-based IoT trading and business model are illustrated in [4]. Using blockchain not only eliminates the need for human interaction but also decreases the cost of developing a payment model for

specific services. Meanwhile, blockchain architecture can help to provide service and name discovery in the IoT system [4]. The proposed blockchains can be abstracted into multiple layers: the service regulators layer (government, organizations), the service providers layer, and the users layer. The regulator layer defines services and, for each service, corresponding service providers act as blockchain peers inside this layer. Similarly, all the devices used for a particular service are registered as blockchain peers in the service provider layer. At the user layer, one could discover, locate, pay for, and access a service without knowing IP or MAC addresses of the related devices. In short, blockchain enables the reliable regulating, payment, and logging for the IoT services.

– **Device management:** As the system owner needs to deploy and maintain a large number of objects with appropriate network and software configurations, the management of all these devices in the IoT system is challenging. Samaniego [4] and Sharma et al. [4] introduced the design of combining blockchain and software-defined networking (SDN) to address the networking management for all the devices. SDN is considered to be an appropriate technique that effectively improves the efficiency of the networking configurations. However, in a large-scale SDN-enabled system, a notable problem is the asynchronous status of the flow rule table. By adding a blockchain layer over the SDN, the problem can be solved. As the result, the integrated system can perform direct deployment, configuration, and management of IoT components. It not only simplifies the device management but also enables fog computing and edge computing to provide additional usable resources for constraint devices. Moreover, new blockchain-based architecture improves the IoT system's performance and capacity, as it is more efficient, secure, and robust. Managing and maintaining the software and firmware for a huge number of devices are also daunting tasks. The problem becomes especially harder when some of the devices are not secured by design. It is essential to fix and patch the vulnerabilities of the firmware and software before adversaries get advantages from these flaws. Boudguiga et al. use blockchain to provide better availability and accountability for IoT software maintenance. As manufacturers have the responsibility to notify of vulnerabilities and provide updates for the flaws, the blockchain can be used as a platform for manufacturers to update the devices reliably. Lim et al. utilized blockchain to provide data integrity during firmware verification of the IoT devices.

– **Data management:** To refine the data management of IoT, Shafagh et al. and Liu et al. introduced auditable IoT data storage and sharing systems based on blockchain. In their design, the blockchain works as the middleware between the data storage services and the IoT devices. Blockchain does not directly store the original data but maintain the references and access control to the IoT data. Blockchain controls, verifies, records, and protects the storage and usage of the IoT data. The inherent reliability and robustness of blockchain ensures the trust and data security for both users and service providers.

Overall, blockchain is the enabler technique of building a smart management mechanism in IoT systems. Blockchain can enable smart manufacturing, remote maintenance, reliable supply chain management, auditable service, and additional security in IoT infrastructure. In the past few years, many blockchain-based IoT applications emerged in many areas, such as agriculture, energy healthcare, industry, smart cities, smart homes, and transportation.

The following sections briefly introduces the blockchain applications in IoT.

Agriculture:

The use of blockchain in IoT agriculture applications also helps to provide transparency and traceability for crop and food supply chain. Leng et al. proposed to use a blockchain-integrated system to provide transparent and secure transaction recording for agriculture supply chain. Moreover, the rent-seeking and matching of resources can be self-adaptively completed. In addition, since food safety is always a public issue, blockchain- and IoT-based agriculture systems can enable reliable food safety by gathering and exposing information about food production, processing, warehousing, and selling. Tian introduced a method of using RFID and blockchain to enhance food safety. Caro et al. implemented a blockchain-based smart agriculture system, which enables the traceability of agriculture products in the supply chain.

Energy:

Smart grid is a revolutionary technique in the electricity power system that enables efficient and automated management via network connections. IoT is the core component and enabler technology of smart grid. By extracting energy data from smart sensors and meters, efficient energy measurement and management can be performed. However, the smart grid has some limitations in complexity and reliability. As power system complexity increases, managing the system becomes challenging. In addition, the utility companies may face problems with convincing customers of the reliability of meter readings.

Healthcare:

Blockchain is also considered a revolutionary technique for healthcare systems. Blockchain-based healthcare implementations fulfill the urgent demands of availability, security, and transparency or privacy, which already play an important role in clinical trials, healthcare data sharing, electrical patient records (EPRs) management, drug tracking, and healthcare device tracking. Meanwhile, smart healthcare, as the most successful and significant application of IoT, would be more preferable and reliable if it could combine with and get benefits from blockchain technology

Industry:

With the emergence of Industry 4.0, IoT has become the backbone technology of cyber-physical systems (CPS), which enable smart sensing and supermatic operations. In addition, smart manufacturing provides remote machine diagnostics and supply chain management provided by the industrial IoT, which can further be enhanced by blockchain. In-depth surveys of blockchain in the industrial IoT are performed in . Bahga et al. pointed out that blockchain-based industrial IoT can be applied to on-demand manufacturing, smart diagnostics, supply chain management, product certification, and machine to machine (M2M) transactions..

Smart City:

A smart city is an automatic and holistic management and convergence of technology, institutions, and human factors. In the technology vision, IoT is the fundamental and crucial component of the urban-scale information communication technology (ICT) platform. As the blockchain can provide benefits to the IoT infrastructure in many aspects, it is reasonable and necessary to investigate the usage of blockchain for smart city applications.

Smart Home:

IoT applications are beginning to direct modern life toward the fusion of convenience and intelligence, as smart wearables and network-enabled home appliances raise the quality of our daily life to a new level. As in the smart city sector, smart home applications can benefit by leveraging the features of blockchain. Fernandez et al. proposed a design of a Zig Bee based smart power outlet system for smart homes. Applying blockchain to this system allows remote control and automatic monitoring of power use.

Transportation:

The concepts and examples of using blockchain to strengthen the vehicular network are briefly mentioned in the paper[4]. There is no doubt that blockchain can be applied to build or reinforce an intelligent transportation system (ITS). Several solutions and designs have emerged recently in this domain. For instance, IBM introduced a blockchain-based freight transportation solution, which can reduce or eliminate fraud or errors and also improve efficiency and security. Instead of focusing on the supply chain or logistics, some researchers aim to utilize blockchain in smart traveling. A blockchain involved transportation system allows the user to securely and efficiently rent or share a vehicle. In addition, payment to the services and the reputation management of the services can be achieved with smart contracts.

5. Challenges of adopting blockchain in IoT:

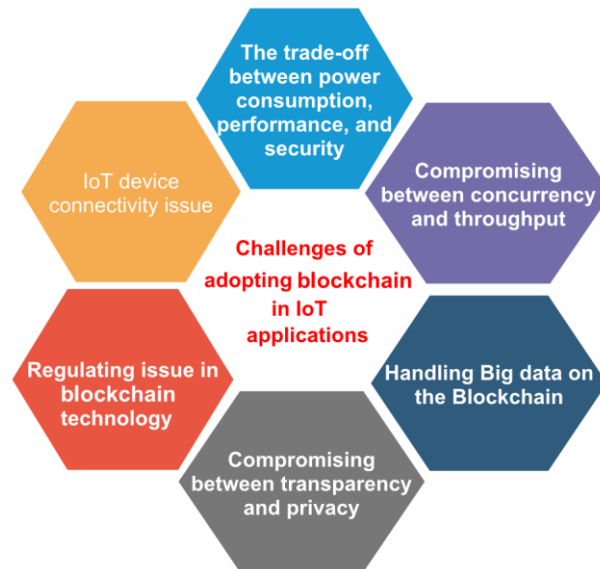


Fig. 4. The challenges of adopting blockchain in IoT (Internet of Things).

Challenge is to boost blockchain's throughput to meet the need of frequent transactions in IoT systems.

Connectivity challenges of IoT: The IoT devices are expected to be connected to high computing storage and networking resources to share IoT data with potential stakeholders. The IoT has limited capabilities to connect them with blockchain technology in order to provide novel business opportunities for the implementation of new applications and services in various domains.

Handling big data on the blockchain: In the blockchain network, every participant maintains a local copy of the complete distributed ledger. Upon the confirmation of a new block, the block is broadcast throughout the entire P2P network, and every node appends the confirmed block to their local ledger. While this decentralized storage structure improves efficiency, solves the bottleneck problem and removes the need for third-party trust, the management of IoT data on the blockchain puts a burden on participants' storage space. The study in Ref. calculated that a blockchain node would need approximately 730 GB of data storage per year if 1000 participants exchange a single 2 MB image per day in a blockchain application. Therefore, the challenge is to address the increasing data storage requirements when blockchain deals with IoT data.

Challenges in maintaining both transparency and privacy: Blockchain can guarantee transparency of transactions, which is essential in some applications like finance. However, user's confidentiality may be adversely affected when storing and accessing IoT data from certain IoT systems such as eHealth on the blockchain. To maintain a balanced degree of transparency and privacy, the development of cost-effective access control for IoT using blockchain is necessary.

Regulating challenges of blockchain in IoT: While several blockchain technological features including decentralization, immutability, anonymity, and automation are promising security solutions for diverse IoT applications, these features combined pose various new regulatory challenges. The immutability feature implies that data is permanently published in distributed transaction ledger (DTL) on the P2P network and cannot be deleted or modified. In addition, due to the absence of governance, records cannot be filtered for maintaining privacy before publishing them on the real world.

6. Conclusion:

In conclusion, this paper has explored the evolving landscape of blockchain and IoT applications, categorizing existing surveys into three main areas. While progress has been made in understanding both technologies individually, limitations persist in their combined use. To address these limitations, our paper offers a fresh perspective, emphasizing blockchain's unique capabilities for enhancing IoT applications. We've provided comparative insights, distilled general integration strategies, and hope these findings will inspire researchers and developers to unlock the full potential of blockchain and IoT, creating more secure and dependable IoT ecosystems.

REFERENCES

- [1] Md Ashraf Uddin, Andrew Stranieri, Iqbal Gondal, Venki Balasubramanian, *A survey on the adoption of blockchain in IoT: challenges and solutions*, 2021.
- [2] Mrs.M.C.Jayaprasanna, Ms.V.A.Soundharya, Ms.M.Suhana, Dr.S.Sujatha, *A Block Chain based Management System for Detecting Counterfeit Product in Supply Chain*, 2021.
- [3] Fei Chen, Zhe Xiao, Laizhong Cui, Qiuzhen Lin, Jianqiang Li, Shui Yu, *Blockchain for Internet of things applications: A review and open issues*, 2020.
- [4] Pinchen Cui, Ujjwal Guin, Anthony Skjellum, David Umphress, *Blockchain in IoT: Current Trends, Challenges, and Future Roadmap*, 2019.
- [5] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, *A Survey on the Security of Blockchain Systems*, 2019
- [6] Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). *A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues*, 2019.
- [7] Wu, M., Lu, Y., Leung, V. C., & Yang, X. *A Comprehensive Survey of Internet of Things (IoT) Enabled by Blockchain 2019*.
- [8] Viriyasitavat, W., Hoonsopon, D., Kantabutra, S., & Kriwattanawong, A, *A Survey of Blockchain for Internet of Things: Applications and Challenges*, 2019.
- [9] Fernandez carames, T. M., & Fraga-Lamas, P, *A Review on the Use of Blockchain for the Internet of Things*, 2018.
- [10] Lo, S. H., Xu, X., Shen, Z., & Feng, C, *Blockchain for Internet of Things: A Survey*, 2018.