International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0204
e ISSN: 2584-2854
Volume: 02
Issue: 05 May 2024
Page No: 1509-1514

Streamlining IoT-driven Data Using Blockchain

Shubham Sharma[1], Tanuja Sharma[2], Akanchha Tiwari[3], Surbhi Gupta[4]
[1,2,3,4]Dept. of IT, Madhav Institute of Technology & Science, Gwalior-MP, India.
Email Id: *shubham6618@outlook.com[1], sharma.tanuja015@mitsgwalior.in[2], tiwariakanchha17@gmail.com[3], surbhigupta968@mitsgwalior.in[4]*

Abstract
The integration of Internet of Things (IoT) technology has revolutionized data collection and analytics, creating vast networks of interconnected devices generating large volumes of data. However, this rapid expansion of IoT ecosystems introduces significant challenges related to data security, integrity, scalability, and privacy. Blockchain technology, with its decentralized and immutable nature, emerges as a compelling solution to address these challenges. This paper explores the synergy between IoT and blockchain, examining how blockchain can streamline IoT-driven data by providing secure data exchanges, enhancing transparency, and facilitating scalability. The study investigates the key mechanisms through which blockchain can mitigate common IoT data issues. It considers blockchain's role in ensuring data integrity by utilizing cryptographic methods, enabling traceability through distributed ledgers, and protecting against unauthorized data manipulation. Furthermore, it explores the potential of blockchain-based smart contracts to automate processes and improve interoperability among IoT devices. The paper delves into specific use cases, such as smart cities, demonstrating how blockchain can effectively streamline IoT data across various industries. The findings highlight that while blockchain offers substantial benefits, it also introduces unique challenges, including high energy consumption, latency concerns, and complex integration processes. This concludes with a discussion of Security concerns, Comparison with existing solutions. By addressing these challenges, blockchain can become a pivotal technology in streamlining IoT-driven data, paving the way for more secure, efficient, and trustworthy IoT ecosystems.
Keywords: *Blockchain; Data Streaming; IoT; IPFS; Smart Contract.*

1. Introduction

The Internet of Things (IoT) has rapidly become a cornerstone of modern technology, enabling a vast array of devices to connect, communicate, and share data. The IoT enables physical devices, automobiles, equipment and even cities are connected to interact with each other and interchange data with the help of embedded sensors [1]. From smart homes and industrial automation to healthcare monitoring and smart cities, IoT's impact is pervasive and transformative. However, this growth has also led to significant challenges in data management, security, and scalability. As IoT networks generate ever-increasing volumes of data, ensuring its reliability, integrity, and confidentiality becomes a complex task. In order to make value from the data generated by the IoT streaming devices, the devices are typically integrated with the cloud or centralized servers for data analysis. This opens a door towards the new paradigm of integrating the IoT with the cloud, creating the Cloud of things [2], [3]. Blockchain technology, originally developed to underpin cryptocurrencies like Bitcoin, has garnered attention for its decentralized, secure, and immutable characteristics [4]. These attributes make blockchain a promising candidate for addressing the inherent challenges of IoT data management. By leveraging blockchain's distributed ledger system, IoT networks can enhance data security, improve transparency, and enable more robust data integrity. Furthermore, blockchain-based smart contracts offer a mechanism for automating processes and establishing trust among disparate IoT devices and stakeholders [5]. This aims to explore how

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0204
e ISSN: 2584-2854
Volume: 02
Issue: 05 May 2024
Page No: 1509-1514

blockchain can streamline IoT-driven data by providing a secure and efficient framework for data exchange, storage, and management [6]. It investigates the key benefits of integrating blockchain with IoT, such as enhanced data security through cryptographic hashing, decentralized consensus mechanisms, and improved data traceability [7]. Additionally, it examines practical use cases across various industries to demonstrate the real-world impact of this integration [8]. Despite its potential, blockchain adoption in IoT systems faces several hurdles, including energy consumption, latency, and the complexity of integrating blockchain into existing IoT architectures [9][10]. This paper will address these challenges and propose potential solutions, highlighting areas for further research and development. By exploring the convergence of blockchain and IoT, this study seeks to contribute to the advancement of secure, scalable, and efficient IoT ecosystems. In summary, this paper provides an overview of the intersection between blockchain and IoT, emphasizing the potential benefits and challenges of this emerging technology combination. Through detailed comparison, it aims to offer insights into how blockchain can streamline IoT-driven data and outline a path toward more secure and efficient IoT networks in the future.

2. Proposed Methodology

The proposed methodology for streamlining IoT-driven data using blockchain and the InterPlanetary File System (IPFS) involves a hybrid approach that combines the immutability and security of blockchain with the distributed file storage capabilities of IPFS. This methodology aims to address the key challenges of IoT data management, including data security, scalability, traceability, and efficient data storage. The proposed architecture consists of three primary components: IoT devices, blockchain infrastructure, and IPFS storage. IoT devices collect data and send it to a blockchain network for secure recording and validation. The actual data content is stored on IPFS, a distributed file system, with the blockchain serving as a ledger for metadata and data hashes to ensure immutability and integrity. The proposed methodology consists of following layers: IoT network layer: Devices in this tier are divided into two classes. Firstly, IoT devices with restricted networking, storage, and processing power. Second, IoT data streaming devices that have sufficient networking, storage, and processing power. Blockchain layer: Using blockchain storage entities, blockchain functions as a decentralized network. Each of these things has an exact duplicate of the whole system. Since IoT data files are frequently massive—many megabytes in size—storing them directly on the blockchain requires a significant amount of throughput and storage capacity. Therefore, the only value kept on the blockchain is the fixed-size hash value, which is several kilobytes. Distributed storage layer: There are difficulties in using blockchain technology to simultaneously ensure privacy and transparency. Comparing IPFS with traditional providers, there are clear benefits. In the first place, it guarantees globally dispersed data storage, avoids node trust, and removes single points of failure. IPFS file archiving and retrieval is similar to web procedures. Similar to URLs, uploaded files are assigned unique hash identities. In contrast, blockchain file storage places a higher priority on transparency, making it unsuitable for huge data. As a result, this study uses SCs to store data off-chain for public blockchain and retrieval. IPFS uses blockchain SCs to provide file access after authentication when users request actions on particular resources. IoT devices, equipped with various sensors, collect data from their respective environments. This data is preprocessed at the edge, which includes data filtering, compression, and encryption. The preprocessing step ensures that only relevant and secure data is sent to the blockchain network, reducing the overall data load and preserving confidentiality. Once data is collected and preprocessed, it is stored in IPFS, which uses a distributed hash table (DHT) to ensure efficient retrieval and sharing. Each stored file or data block on IPFS is assigned a unique hash, which is a cryptographic representation of the data's content. This hash serves as an identifier and ensures data

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0204
e ISSN: 2584-2854
Volume: 02
Issue: 05 May 2024
Page No: 1509-1514

immutability and traceability. The blockchain component acts as a secure ledger, storing metadata related to the IoT data stored in IPFS. For each data block stored in IPFS, a corresponding transaction is created on the blockchain. This transaction contains the IPFS hash, timestamp, and relevant metadata (e.g., device ID, data type, location). This structure allows the blockchain to serve as a source of truth for the data's provenance and ensures the integrity and authenticity of the data. Smart contracts are deployed on the blockchain to automate processes and enforce data access policies in Figure 1.

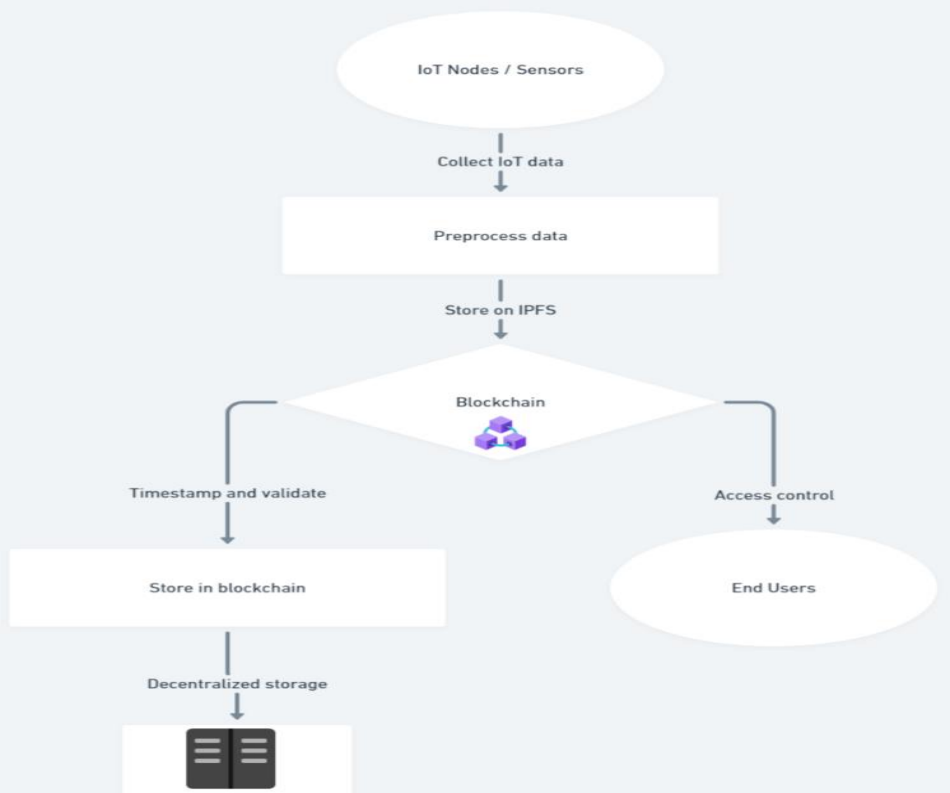

Figure 1 System Diagram Streamlining of IOT Driven Data Using Blockchain

These contracts can be used to define conditions for data sharing, such as user permissions, device authentication, and data retention policies. Additionally, smart contracts can automate workflows, such as triggering alerts or notifications when specific conditions are met in the IoT data. To retrieve data, users or applications query the blockchain to obtain the relevant IPFS hashes. Using these hashes, the data can be quickly retrieved from IPFS. The blockchain's distributed ledger ensures that the retrieved data is verified for integrity and authenticity, as any tampering with the data would result in a mismatch with the stored hash. Security and privacy are paramount in this methodology. Blockchain's decentralized and cryptographic nature ensures data integrity and resistance to tampering. Data stored on IPFS can be encrypted to protect sensitive information, and access control mechanisms can be implemented through smart contracts. Additionally, the distributed nature of IPFS reduces single points of failure, enhancing overall system reliability.

3. Results and Discussion

The integration of blockchain and the InterPlanetary File System (IPFS) into the Internet of Things (IoT) ecosystem offers a compelling solution to many of the challenges inherent in IoT data management. This discussion focuses on two key areas: security

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0204
e ISSN: 2584-2854
Volume: 02
Issue: 05 May 2024
Page No: 1509-1514

analysis and a comparison with existing solutions, incorporating insights from relevant research.

3.1. Security Analysis

One of the primary concerns in IoT is ensuring the security and integrity of data as it moves through the system. Blockchain and IPFS provide robust mechanisms to address these issues.

Blockchain's inherent immutability, achieved through cryptographic hashing and consensus mechanisms, ensures that once data is recorded, it cannot be altered without detection. This characteristic is crucial for maintaining data integrity in IoT applications, especially those with compliance and audit requirements. IPFS complements this by providing a distributed file system where data blocks are hashed, guaranteeing their integrity. This dual-layer approach significantly reduces the risk of data tampering. Blockchain's decentralized nature inherently resists single points of failure, as multiple nodes maintain copies of the ledger. This structure reduces the risks associated with centralized systems, where a single breach could compromise the entire system. IPFS further enhances this decentralization by distributing file storage across a peer-to-peer network, reducing data loss risk from server outages or targeted attacks. Encryption plays a central role in protecting data within IoT systems. With blockchain and IPFS, sensitive data can be encrypted before storage, ensuring that only authorized parties can access it. Smart contracts can enforce access controls, ensuring that data is shared only with entities that meet predefined conditions. This level of automation adds an additional layer of security, reducing human error and potential security gaps. Blockchain-based identity verification and authentication mechanisms provide a secure method for ensuring that only trusted devices and users can interact with the system. Smart contracts can be used to implement complex authorization policies, allowing fine-grained control over who can access and modify data. These mechanisms significantly reduce the risk of unauthorized access and data breaches.

3.2. Comparison with Existing Solutions

In the context of IoT data management, existing solutions often rely on centralized architectures or traditional distributed databases. Following are Comparison on blockchain and IPFS with these existing approaches, using relevant research for context in Table 1.

Table 1 Comparison with Existing Solutions

APPROACH	DESCRIPTION	STORAGE	BLOCKCHAIN ROLE	PRIVACY
[11]	Decentralized access management system for IoT devices.	CoAP is used and data is privately stored on a network accessible storage.	Access management using an Ethereum blockchain.	Private blockchain
[12]	Blockchain-based solution for sharing weather sensor data in a marketplace. NTUA token is used.	Maria database is used for blockchain events. Weather sensor data is stored on centralized server.	Ethereum blockchain for events and access management	Users with provided key can access the requested data
[13]	Generic blockchain-based solution for access control	Off-chain storage	Access control and identity management of data	Encryption of data

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0204
e ISSN: 2584-2854
Volume: 02
Issue: 05 May 2024
Page No: 1509-1514

[14]	Distributed access control and management system of IoT data	Cloud storage or decentralized storage	Management and access control of data	Encryption using key
[15]	Decentralized access model for IoT data using a consortium architecture	InterPlanetary File System	Smart contract access control on stored keys	Hashes are encrypted
Proposed Solution	Blockchain based decentralized solution for streamlining IoT driven data	InterPlanetary File System	Access control based on Smart contract, an immutable trusted ledger for chunks hash sharing.	Hashes are encrypted

Conclusion

This proposed methodology provides a comprehensive approach to streamlining IoT-driven data using blockchain and IPFS. By combining the strengths of blockchain's immutability with IPFS's distributed file storage, this approach addresses the key challenges of IoT data management, offering enhanced security, scalability, and data integrity. The use of smart contracts further automates processes and ensures efficient data access control. Future work will involve testing and validating this methodology across various IoT use cases to demonstrate its effectiveness in real-world scenarios.

References

[1]. C. Stergiou, K. E. Psannis, B.-G. Kim, and B. Gupta, "Secure integration of iot and cloud computing," Future Generation Computer Systems,vol. 78, pp. 964–975, 2018.

[2]. A. Alli and M. M. Alam, "The fog cloud of things: A survey on concepts, architecture, standards, tools, and applications," Internet of Things,vol. 9, p. 100177, 2020.

[3]. M. M. Mahmoud, J. J. Rodrigues, S. H. Ahmed, S. C. Shah, J. F.Al-Muhtadi, V. V. Korotaev, and V. H. C. De Albuquerque, "Enabling technologies on cloud of things for smart healthcare," IEEE Access, vol. 6,pp. 31 950–31 967, 2018.

[4]. Banafa, "Iot and blockchain convergence: benefits and challenges," IEEE Internet of Things, 2017.

[5]. Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," International Journal ofWeb and Grid Services, vol. 14, no. 4, pp. 352–375, 2018.

[6]. Kummar, S., Bhushan, B. & Bhatia, S. Blockchain based big data solutions for Internet of Things (IoT) and smart cities. In New Trends and Applications in Internet of Things (IoT) and Big Data Analytics (eds Sharma, R. & Sharma, D.) 225–253 (Springer International Publishing, Cham, 2022). https:// doi. org/ 10. 1007/ 978-3- 030- 99329- 0_ 15.

[7]. Pradhan, N. R. & Singh, A. P. Smart contracts for automated control system in blockchain based smart cities. J. Ambient Intell. Smart Environ. 13(3), 253–267 (2021).

[8]. Hilbig, A., Lehmann, D., Pradel, M., An empirical study of real-world webassembly binaries: Security, languages, use cases. In Proceedings of the Web Conference 2021, 2696–2708, (2021)

[9]. Shahid, A. R., Pissinou, N., Staier, C., Kwan, R. Sensor-chain: A lightweight scalable

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0204
e ISSN: 2584-2854
Volume: 02
Issue: 05 May 2024
Page No: 1509-1514

blockchain framework for internet of things. In 2019 International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 1154–1161, (2019)

[10]. Khan, S., Lee, W.-K., Majeed, A. & Hwang, S. O. Blockchain meets lightweight cryptography. IEEE Potentials 41(6), 38–42 (2022).

[11]. O. Novo, "Blockchain meets iot: An architecture for scalable access management in iot," IEEE Internet of Things Journal, vol. 5, no. 2, pp.1184–1195, 2018.

[12]. G. Papadodimas, G. Palaiokrasas, A. Litke, and T. Varvarigou, "Implemen-tation of smart contracts for blockchain based iot applications," in 2018 9th International Conference on the Network of the Future (NOF). IEEE,2018, pp. 60–67.

[13]. S. Bajoudah, C. Dong, and P. Missier, "Toward a decentralized, trust-less marketplace for brokered iot data trading using blockchain," in 2019 IEEE international conference on blockchain (Blockchain). IEEE, 2019, pp. 339–346.

[14]. H. Shrobe, D. L. Shrier, and A. Pentland, "Enigma: Decentralized computation platform with guaranteed privacy," 2018.

[15]. H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, "Towards blockchain-based auditable storage and sharing of iot data," in Proceedings of the 2017 on cloud computing security workshop, 2017, pp. 45–50.