RESEARCH ARTICLE WWW.PECEJOURNAL.COM

Transforming Smart Devices and Networks using Blockchain for IoT

Lau W. Cheng[1], **Beh L. Wei**[2]

[1,2]*Faculty of Information Science and Technology University, Kebangsaan, Malaysia*

KEYWORDS:
Blockchain;
Internet of Things (IoT);
Smart Devices;
Decentralized Networks;
Security;
Smart Contracts;
Data Integrity

ARTICLE HISTORY:
Received : 18.11.2024
Revised : 24.12.2024
Accepted : 13.03.2025

https://doi.org/10.31838/ECE/02.01.06

Abstract

Blockchain technology holds transformative potential for the Internet of Things (IoT), offering enhanced security, transparency, and efficiency for smart devices and networks. As IoT ecosystems proliferate, they encounter significant challenges, including data integrity, security vulnerabilities, and centralized control. Blockchain's decentralized ledger technology addresses these issues by ensuring tamper-proof data records, enabling secure peer-to-peer communication, and eliminating reliance on central authorities. Smart contracts, programmable and self-executing contracts on the blockchain, facilitate automated interactions between IoT devices, streamlining processes and reducing human intervention. Furthermore, blockchain enhances device authentication and authorization, mitigating risks of unauthorized access and cyber-attacks. The synergy between blockchain and IoT promotes more resilient, autonomous, and trustworthy networks, fostering innovations in various sectors, such as healthcare, supply chain, and smart cities. However, the integration of blockchain with IoT also presents challenges, including scalability concerns, energy consumption, and the need for new standards and protocols. Ongoing research and development aim to overcome these hurdles, paving the way for the widespread adoption of blockchain-enabled IoT systems. Ultimately, blockchain technology is poised to revolutionize IoT by creating more secure, efficient, and interoperable smart environments.

Author's e-mail: Lau.wai@ftsm.ukm.my, beh.lee@ftsm.ukm.my

How to cite this article: Cheng LW, Wei BL. Transforming Smart Devices and Networks using Blockchain for IoT, Journal of Progress in Electronics and Communication Engineering Vol. 2, No. 1, 2025 (pp. 60-67).

Introduction

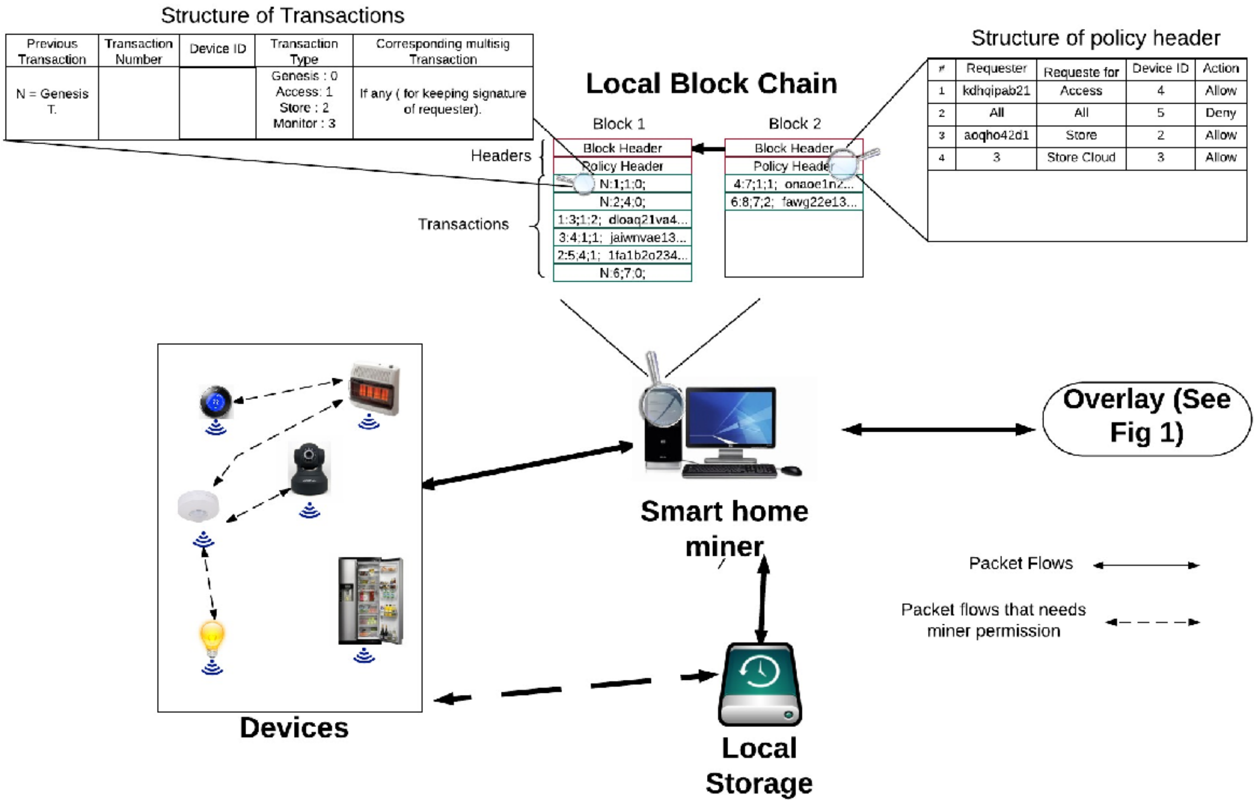
The Internet of Things (IoT) is revolutionizing the way we interact with devices and networks, enabling seamless connectivity and data exchange on an unprecedented scale.[1] However, as the number of connected devices continues to grow, concerns over security, transparency, and trust become increasingly paramount.[2] This is where blockchain for IoT emerges as a transformative solution, offering an immutable and decentralized ledger that ensures the integrity and traceability of transactions across smart devices and networks.[1-3]

By harnessing the power of blockchain technology, businesses can leverage the added security, accountability, and trust that comes with sending IoT data to private blockchain networks.[1-2] Each transaction is recorded, verified, and added to an immutable chain, preventing disputes and fostering trust among all authorized network members.[1-3] Moreover, the open and interoperable nature of blockchain platforms, like IBM's, provides flexibility and adaptability for a multicloud world, paving the way for seamless integration with cutting-edge technologies like the IBM Watson IoT Platform.[1]

A. Preliminaries

Blockchain is a distributed, decentralized database that maintains an immutable and transparent record of transactions or digital events across a network of participants.[5-8] It operates without a central authority, relying instead on a consensus mechanism to validate and secure each new block of data added to the chain.[7] The blockchain technology offers significant advantages such as non-tampering, non-forgery, and traceability, making it an ideal solution for storing and securing critical data.[8]

The concept of blockchain originated with the introduction of Bitcoin, the first decentralized cryptocurrency, in 2008.[6] Bitcoin utilizes the blockchain



Structure of Transactions

Previous Transaction	Transaction Number	Device ID	Transaction Type	Corresponding multisig Transaction
N = Genesis T.			Genesis : 0 Access: 1 Store : 2 Monitor : 3	If any (for keeping signature of requester).

Structure of policy header

#	Requester	Requeste for	Device ID	Action
1	kdhqipab21	Access	4	Allow
2	All	All	5	Deny
3	aoqho42d1	Store	2	Allow
4	3	Store Cloud	3	Allow

Fig. 1: Blockchain for IoT security and privacy

to record and verify transactions in a peer-to-peer network without the need for a central authority or intermediary.[5-6] Each transaction is secured through cryptographic proof and digital signatures, ensuring the integrity and authenticity of the data.[5]

In a blockchain network, data is distributed across millions of computers or nodes worldwide, eliminating the need for a central server or system.[5] This decentralized architecture enhances the security and resilience of the network, as there is no single point of failure.[7] Nodes in the network validate and propagate transactions onto the blockchain, with miners or validators earning incentives for their contributions.[5-7]

B. Consensus Algorithms

A consensus algorithm is a critical component of any blockchain network, responsible for achieving agreement among the nodes regarding the current state of the distributed ledger.[7] It establishes trust and reliability within the network, ensuring that every new block added to the blockchain is the authoritative and agreed-upon version of the truth.[7]

Various consensus algorithms have been developed to address different requirements and trade-offs within blockchain networks. Some of the most widely used consensus algorithms include:

1. **Proof of Work (PoW):** Used in Bitcoin, PoW requires miners to solve complex mathematical puzzles through computational power to validate transactions and create new blocks.[7] The miner who solves the puzzle first earns the right to add the next block and receive a reward.[7]
2. **Proof of Stake (PoS)**: An alternative to PoW, PoS requires validators to stake or lock up a portion of their cryptocurrency holdings to participate in the validation process.[7]. Validators are selected based on their economic stake in the network, and rewards are distributed proportionally.[7]
3. **Practical Byzantine Fault Tolerance (PBFT):** This consensus algorithm is designed to handle Byzantine faults, where some nodes in the network may behave maliciously or fail unexpectedly.[7] PBFT ensures that the network can reach consensus even in the presence of faulty nodes.[7]
4. **Delegated Proof of Stake (DPoS):** In this variant of PoS, users delegate their voting power to representatives or witnesses, who are responsible for validating transactions and creating new blocks.[7] Rewards are distributed to both witnesses and delegators.[7]

5. **Proof of Burn (PoB):** Validators in PoB "burn" or send a portion of their cryptocurrency to an unrecoverable address, earning the privilege to mine based on a random selection process.[7] The more coins burned, the higher the chance of being selected as a validator.[7]
6. **Proof of Elapsed Time (PoET):** PoET is a fair consensus algorithm used in permissioned blockchain networks, where each validator has an equal chance to create a new block based on a random waiting time.[7] Additional checks prevent nodes from consistently winning or generating the lowest timer values.[7]

These consensus algorithms aim to achieve agreement, collaboration, and cooperation among nodes while ensuring the integrity and security of the blockchain network.[7] The choice of consensus algorithm depends on factors such as network requirements, scalability, energy efficiency, and decentralization.[7]

Related work

The integration of blockchain technology with the Internet of Things (IoT) has garnered significant attention from researchers and industry professionals alike. The decentralized and secure nature of blockchain makes it an attractive solution for addressing the privacy and security challenges associated with IoT devices and networks.[8-10]

A. Decentralized and Private-by-Design IoT

Researchers have explored the potential of combining blockchain and peer-to-peer (P2P) approaches to foster a decentralized and private-by-design IoT ecosystem. The goal is to leverage the blockchain's immutability and transparency to register and authenticate all operations performed on IoT device data, while leveraging P2P storage systems to ensure privacy, robustness, and the absence of single points of failure.[11]

A private-by-design IoT could be fostered by combining blockchain and a P2P storage system, where sensitive data produced and exchanged among IoT devices are stored in the P2P system, ensuring privacy and resilience. The blockchain would play a fundamental role in registering and authenticating all operations performed on this IoT device data.[12]

To validate this approach, researchers have conducted Systematic Literature Reviews (SLRs) to investigate documented use cases in the state of the art and identify the main factors affecting the levels of integrity, anonymity, and adaptability of the blockchain in such scenarios.[13]

B. Authentication Schemes for Smart Cities

The integration of blockchain technology with IoT has also been explored in the context of smart city architectures, particularly for authentication schemes. Researchers have reviewed and analyzed existing security services, challenges, and issues related to authentication in smart cities.[14-15]

1. **Traditional Authentication Schemes:** Early adoption of traditional state-of-the-art authentication schemes for IoT-enabled smart assets in smart cities has been studied to reveal their full potential.
2. **Blockchain-enabled Authentication:** Comprehensive classifications and detailed reviews of the latest authentication schemes for IoT-enabled smart assets in smart cities, based on centralized and distributed blockchain-enabled architectures, have been conducted.
3. **Blockchain-as-a-Service:** The concept of Blockchain-as-a-Service has emerged as a result of reviewing existing solutions and discussing related challenges and issues in smart cities.
4. **Evaluation and Analysis:** Researchers have identified and discussed the pros and cons of existing authentication schemes in smart city architectures, providing insights into their suitability and potential improvements.

C. Blockchain Implementation and Applications

Beyond the specific applications of blockchain in IoT and smart cities, researchers have also explored the broader implementation of blockchain technology across various domains.[16-18]

1. **Research Discussions:** In recent years, the implementation of blockchain technology for various applications has been widely discussed in the research community and industry.
2. **Application Areas:** Numerous articles have discussed the possibility of applying blockchain technology in areas such as healthcare, IoT, and business.
3. **Ecosystem Analysis:** Research studies have presented complete ecosystems of blockchain, summarizing and analyzing the various aspects covered in the reviewed papers.
4. **Platform Analysis:** Analyses have been performed on various blockchain platforms, their consensus models, and applications, providing insights into the strengths and limitations of different blockchain implementations.

These research efforts highlight the growing interest and exploration of blockchain technology in various domains, including IoT and smart cities, with a focus on addressing challenges related to security, privacy, and decentralization.

BLOCKCHAIN BASED DISTRIBUTED IOT DATA STORAGE FRAMEWORK

This section introduces a four-layered architectural design for a transparent and secure IoT data-sharing framework as depicted in Fig. 2. These layers function autonomously and in a decentralized manner for computation and storage administration [19]-[20]. The main objective of the framework is to enable blockchain scalability in terms of transaction throughput and latency. The overall goal is to extricate the blockchain ledger from the extra burden of millions of local transactions within IoT networks.[21]

A. IoT network layer

This layer devices are categorized into two groups. First, constrained IoT devices with limited computing power, storage, and networking capabilities. Secondly, IoT data streaming devices with adequate computing power, storage, and networking capabilities. It can be noticed from Fig. 2, IoT streaming devices can interact directly with SC and upload data to storage and they do not need any external devices to ease such interaction. They can also communicate with the storage components directly. However, the other constrained IoT devices rely on smart gateways to communicate with the blockchain, they can bridge the gap between their limited capabilities of the blockchain SCs.

It also comprises a consensus node and an IoT node. IoT nodes which collect data from the surroundings. They send data to the local blockchain at user-defined intervals. On the other hand, consensus nodes collect data like IoT nodes and also enforce consensus algorithms like DPoS. These nodes are generally powered by a main source and not restricted by high computational requirements due to the DPoS consensus algorithm. Additionally, local blockchains efficiently handle and process transactions within the network. The local blockchain operates within the IoT gateways with blockchain capabilities with primary functions that include maintaining a lightweight backup of the public blockchain and serving as a registry. Whenever a new block joins the public blockchain, the local blockchain only retains key details such as the

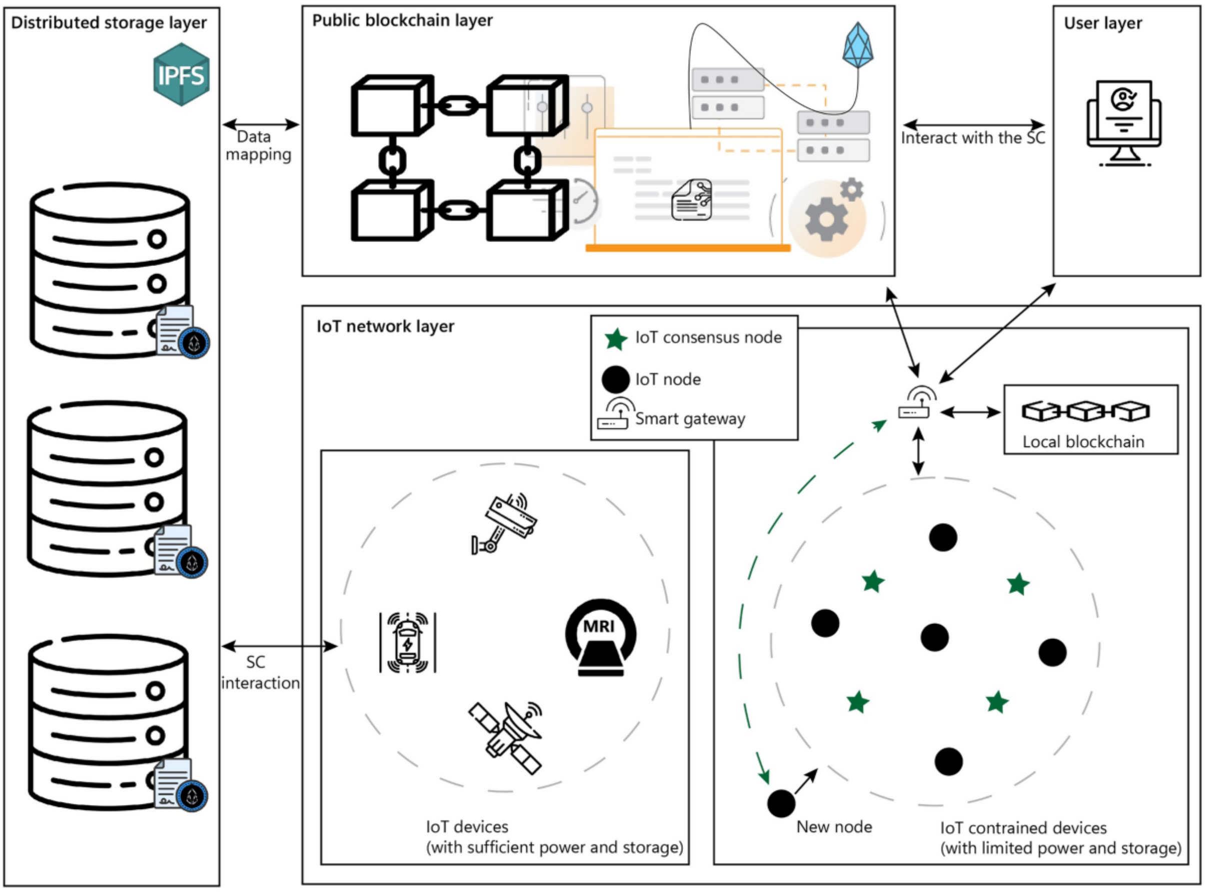


Fig. 2: A scalable blockchain

total data packet count, validator node ID, and the new block address. The actual data block is stored within the public blockchain. When a new node seeks to join the IoT network, the gateway facilitates communication with consensus IoT nodes. From the pool of available nodes, a validator IoT node distinguished by its robust computational power and operation is selected.

B. Public blockchain layer

The public blockchain operates as a decentralized network comprising blockchain storage entities. Each of these entities possesses a comprehensive replica of the entire system. This approach ensures system resilience in case a significant number of network nodes become inaccessible, and data is lost. The entire system can be reconstructed using a single node that maintains a complete copy of the blockchain.

The implementation of the SC takes place at the public blockchain layer. The SC functionalities are specifically designed for the IoT ecosystem, such as the registration of new IoT nodes and facilitating communication between the public blockchain and gateway. By employing a SC, the interaction process between the gateway and the public blockchain becomes automated and secure. Since the SC resides on the blockchain, it is not possible to upgrade or introduce new features to the source code directly. If there arises a need to incorporate additional functionalities into the SC in the future it can only be achieved by modifying and relaunching an updated version of the SC on the blockchain. Upon deployment of the new contract on the blockchain, entities within the proposed system are mandated to utilize the hash address of the new SC for accessing its extended functionalities.[16-21]

This element essentially operates as a blockchain-based database that stores SHA-256 hashes of IoT- generated data, along with the corresponding URL hash pointer. This arrangement guarantees that the specific details of the data remain private and inaccessible to the public, thus safeguarding individuals' privacy. Furthermore, given that IoT data files are typically large, spanning several megabytes, storing them directly on the blockchain necessitates substantial throughput and storage resources. Hence, only the fixed-size hash value amounting to several kilobytes is stored on the blockchain.

C. Distributed storage layer

Ensuring both privacy and transparency through blockchain simultaneously presents challenges.[21] Specifically, the storage of raw data on the blockchain raises significant privacy and scalability concerns. To address this, the research employs a combination of off-chain storage and on- chain verification to achieve both privacy and authenticity at once.

The main responsibility for storing the complete record set rests with off-chain storage, realized through the implementation of the IPFS protocol. IPFS is a peer-to-peer distributed protocol aims to unify computing devices into a single file system mitigating the risk of a single point of failure. Streaming IoT data with sufficient computational power and storage can be uploaded directly to the IPFS. Unlike previous peer-to-peer systems such as BitTorrent, Git, Self-certified File Systems, and distributed hash tables, IPFS provides a comprehensive framework for the distributed sharing of extensive datasets. Moreover, IPFS provides a storage solution supporting large data volumes and utilizing content-based hyperlinks.

D. User layer

End users can interact with the gateway to obtain the desired IoT data as the gateway also retains the local blockchain data. However, if the user retrieves data from the streaming IoT devices it can be relatively large in size. As, the IoT data stream is chunked based on a sampling period is transferred by the IoT devices off-chain (distributed) for storage, and on-chain (public blockchain) only their details (chunk number, timestamped index, hash) are transferred through the SC. Hence, it is clear to see that the requirements are undoubtedly different. For this purpose, data can be retrieved from the on-chain.

Performance evaluation

A. Latency and Throughput

The performance evaluation of the proposed blockchain-based IoT framework primarily focuses on assessing latency and throughput. Latency measures the time it takes for a data packet to reach the gateway and become part of the blockchain. A higher latency value indicates greater difficulty in adding data packets to blocks, hindering the efficient expansion of the IoT blockchain framework.[21] The throughput metric, on the other hand, is measured in terms of the number of successful transactions, starting from the first transaction deployed until the last chain transaction. It demonstrates the system's ability to handle an increasing number of blockchain IoT nodes per gateway.[22]

Figure 3 illustrates the observed trends in the latency of accepting a single data packet. When using the Proof-of-Stake (PoS) consensus algorithm, the latency

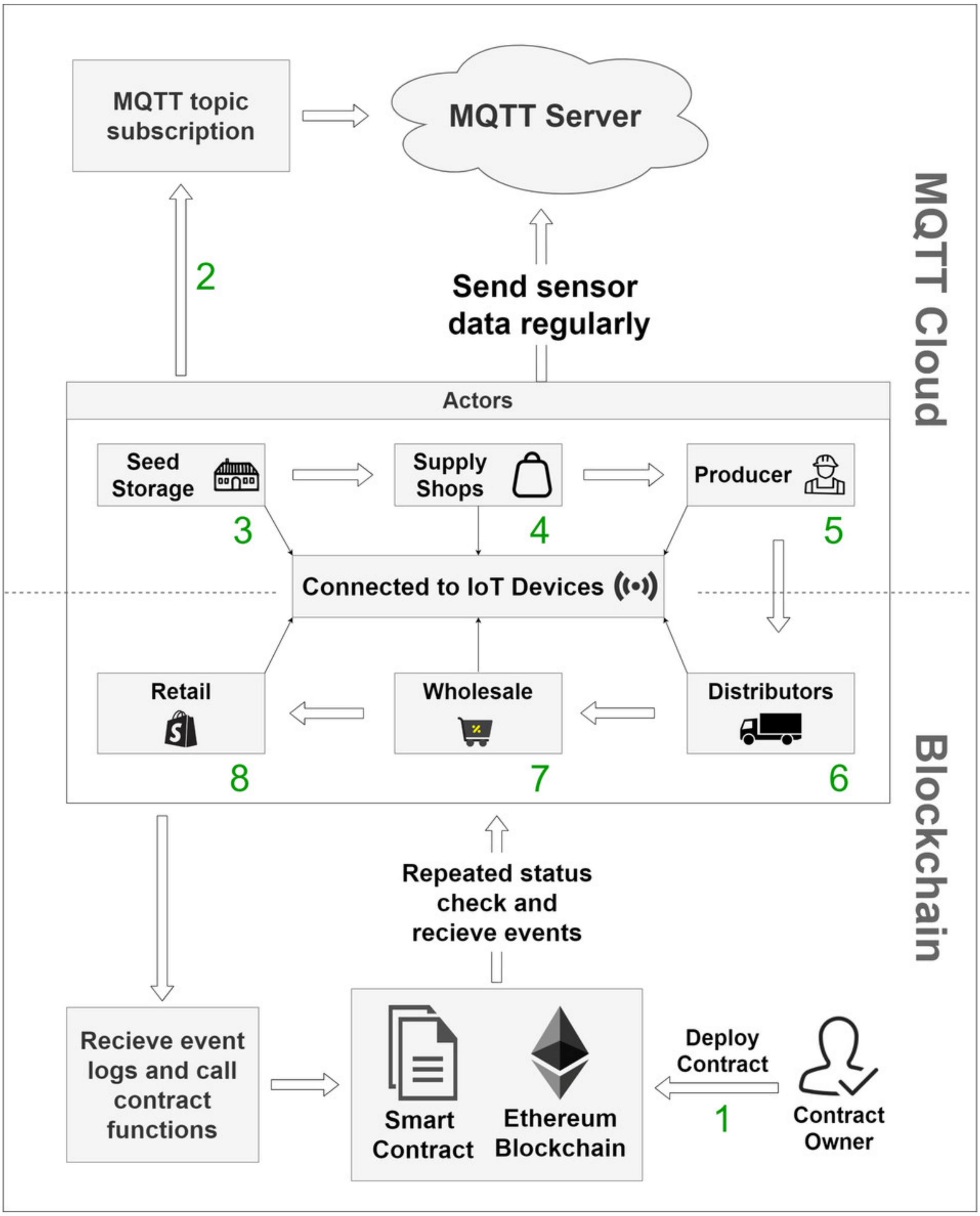


Fig. 3: Blockchain and smart contract for IoT

for accepting a data packet increases. For instance, the latency for 500 nodes in the PoS approach is 55.4 ms, while the latency in the Delegated Proof-of-Stake (DPoS) approach is 0.976 ms.[26] This discrepancy arises because a small number of elected delegates validate and confirm transactions in the DPoS approach, while the PoS validation process for an individual data packet is prolonged due to the absence of instantaneous execution and a larger validation pool. Consequently, these data packets are queued for validation and subsequent addition to blocks, resulting in a prolonged validation process for each individual data packet.[23]

The results of the throughput metric are demonstrated in Fig. 4. It is evident that the DPoS approach outperforms the PoS-based approach in terms of transaction processing efficiency. For instance, in a scenario where 20,000 nodes are sending transactions, the throughput

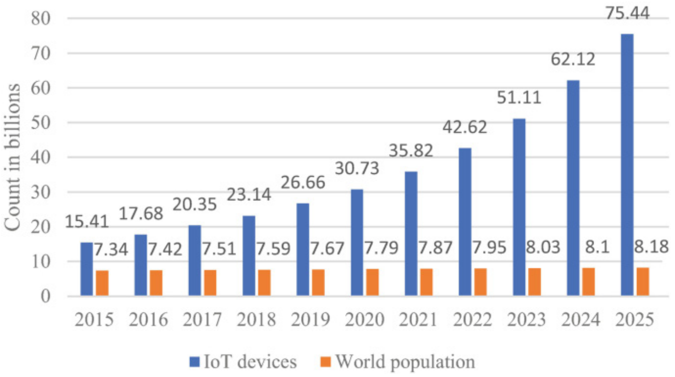


Fig. 4: AI, Blockchain, and IOT

reaches its maximum with the DPoS-based approach as the framework copes with an increasing number of blockchain IoT nodes. In contrast, the PoS-based approach processes a lower number of transactions, reaching 16,006.73.[24] This discrepancy arises because the PoS approach becomes saturated before achieving a higher throughput.

B. Resource Consumption

The results in Fig. 5 are presented to examine the impact of network (*NET*) and CPU resources. In this experiment, the range of IoT nodes was varied from 500 to 20,000 to gauge the effect on *NET*/*CPU*. Fig. 5 shows that the CPU usage is 1.136 ms for 500 nodes, and when set to 20,000 nodes, it almost reaches 27.326 ms.[21] Figure 5 also reveals a consistent value of 104 for *NET* bandwidth, indicating no variations. This constancy has minimal impact on bandwidth, primarily due to the size of the data packet.[22]

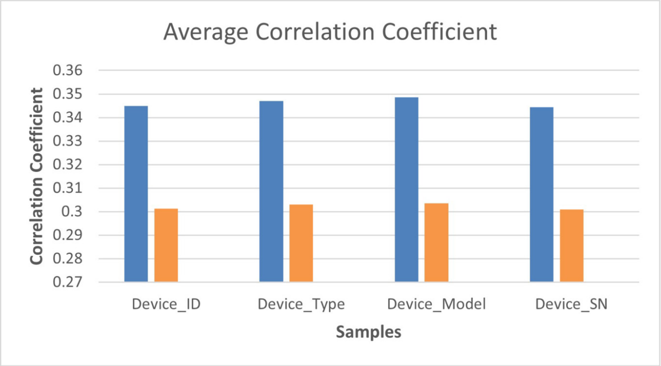


Fig. 5: Utilizing Blockchain for IoT Privacy through Enhanced ECIES

C. Scalability

The outcomes are noticeable through the analysis of Figs. 3, 4, and 5. As illustrated in Fig. 3, upon increasing the number of blockchain IoT nodes, the latency under the PoS-based approach approximately increases exponentially.[22] Furthermore, it becomes evident in Fig. 4 that the throughput observed within the DPoS-based approach transaction speed has good linear scalability when the number of nodes increases. For instance, when 500 nodes engage in transactional activities, the DPoS-based approach achieves a throughput of 500 TPS, while the PoS-based approach records a throughput of 496.31 TPS.[22] This demonstrates that the DPoS approach outperforms the PoS approach and performs well when the number of blockchain IoT nodes increases.

D. IPFS Storage Efficiency

In the realm of the public network environment, a comprehensive analysis was undertaken to evaluate the upload time and speed of the InterPlanetary File System (IPFS) (https://ipfs.tech/). The system configuration encompassed specifications of 8 GB memory, 2 cores, and an 8 MB bandwidth. As seen in Table 2, the upload speed exhibited consistent stability, maintaining an approximate rate of 7 MB/s.[24]

Figure 6 depicted that the file hash was uploaded and retrieved from on-chain. It was observed that the upload time is relatively large compared to retrieving the hash. This is because it stores the content identifier on-chain during uploading, while during retrieval, it only verifies the node making the request [24]. These findings strongly support the widespread adoption and promotion of IPFS in the field of distributed storage applications.

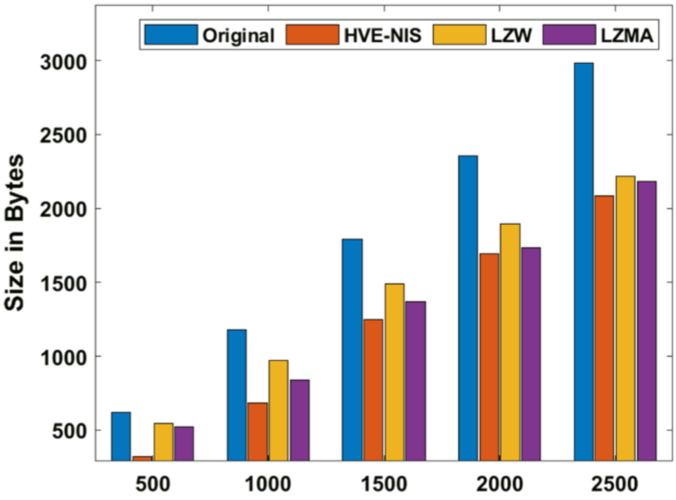


Fig. 6: Internet of things-based secure healthcare framework

Conclusion and Future Work

The blockchain technology offers a revolutionary approach to address the challenges of security, transparency, and trust in the Internet of Things (IoT) ecosystem. By leveraging its decentralized architecture and immutable ledger, blockchain enables secure data sharing, robust authentication mechanisms, and tamper-proof record-keeping for IoT devices and networks. The proposed four-layered framework seamlessly integrates blockchain with distributed storage solutions like IPFS, facilitating scalability, privacy, and efficient data management.The performance evaluation of the framework highlights the superiority of the DPoS consensus algorithm over the traditional PoS approach in terms of latency, throughput, and scalability. The resource consumption analysis further validates the framework's efficiency, showcasing minimal impact on network bandwidth. Additionally, the incorporation of IPFS demonstrates promising upload and retrieval speeds, underscoring its suitability for distributed storage applicati ons. As IoT continues to proliferate, the synergy between blockchain and emerging technologies will pave the way for secure, transparent, and trustworthy smart device networks.

References

1. Christidis, K., &Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. IEEE Access, 4, 2292-2303.
2. Selvam, L., et al. "Collaborative autonomous system based wireless security in signal processing using deep learning techniques." Optik 272 (2023): 170313.
3. Rani, B. M. S., et al. "Disease prediction based retinal segmentation using bi-directional ConvLSTMU-Net." Journal of Ambient Intelligence and Humanized Computing (2021): 1-10.
4. Atzori, L., Iera, A., & Morabito, G. (2010). The Internet of Things: A survey. Computer Networks, 54(15), 2787-2805.
5. Dorri, A., Kanhere, S. S., Jurdak, R., &Gauravaram, P. (2017). Blockchain for IoT security and privacy: The case study of a smart home. In 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops) (pp. 618-623). IEEE.
6. Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A review on the use of blockchain for the internet of things. IEEE Access, 6, 32979-33001.
7. Benet, J. (2014). Ipfs-content addressed, versioned, p2p file system. arXiv preprint arXiv:1407.3561.
8. Nizam, Taaha, et al. "Novel all-pass section for high-performance signal processing using CMOS DCCII." TENCON 2021-2021 IEEE Region 10 Conference (TENCON). IEEE, 2021.
9. Babu, D. Vijendra, et al. "Digital code modulation-based MIMO system for underwater localization and navigation using MAP algorithm." Soft Computing (2023): 1-9.
10. Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180-184). IEEE. [31]
11. Wilkinson, S., Boshevski, T., Brandoff, J., Prestwich, J., Hall, G., Gerbes, P., ... &Buterin, V. (2014). Storj a peer-to-peer cloud storage network.
12. Loeliger, J., & McCullough, M. (2012). Version control with git: Powerful tools and techniques for collaborative software development. O'Reilly Media, Inc.
13. Pittala, C.S., et al., "1-Bit FinFET carry cells for low voltage high-speed digital signal processing applications," Silicon, 15(2), 2023, pp.713-724.
14. Rani, B.M.S., et al., "Road Identification Through Efficient Edge Segmentation Based on Morphological Operations," Traitement du Signal, 38(5), 2021.
15. Buterin, V. (2014). A next-generation smart contract and decentralized application platform. white paper, 3(37).
16. Dwork, C., &Naor, M. (1992). Pricing via processing or combatting junk mail. In Annual International Cryptology Conference (pp. 139-147). Springer, Berlin, Heidelberg.
17. Jakobsson, M., &Juels, A. (1999). Proofs of work and bread pudding protocols. In Secure Information Networks (pp. 258-272). Springer, Boston, MA.
18. Haber, S., &Stornetta, W. S. (1991). How to time-stamp a digital document. In Conference on the Theory and Application of Cryptography (pp. 437-455). Springer, Berlin, Heidelberg.
19. Merkle, R. C. (1987). A digital signature based on a conventional encryption function. In Advances in Cryptology—CRYPTO'87 (pp. 369-378). Springer, Berlin, Heidelberg.
20. Spiekermann, S., Acquisti, A., Böhme, R., & Hui, K. L. (2015). The challenges of personal data markets and privacy. Electronic Markets, 25(2), 161-167.
21. Koutroumpis, P., Leiponen, A., & Thomas, L. D. (2020). Markets for data. Industrial and Corporate Change, 29(3), 645-660.
22. ISO/IEC. (2016). ISO 15489-1:2016 – Information and Documentation – Records Management-Part I: General, ISO, Geneva.
23. European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L119, 1-88.
24. Vijay, V. and Srinivasulu, A., "A novel square wave generator using second-generation differential current conveyor," Arabian Journal for Science and Engineering, 42(12), 2017, pp.4983-4990.