Optimized Fusion Chain with Web3 Storage

Tahiya Tabassum Lisa[a] and Chaiyachet Saivichit[b]
Wireless Network and Future Internet Research Unit,
Department of Electrical Engineering, Faculty of Engineering,
Chulalongkorn University, Bangkok 10330, Thailand

Keywords: Fusion Chain, IoT, Web3 Storage, Practical Byzantine Fault Tolerance Consensus Algorithm, Raft Consensus Algorithm.

Abstract: The Internet of Things (IoT) has become increasingly popular over the past two decades. It has a significant impact on many aspects of daily life, including smart cities, intelligent transportation, manufacturing, and several other industries. Processing and networking abilities of the Internet of Things are condemned/ censorious in today's highly technological environment. These systems are also reasonably priced when used on embedded platforms and consume little power (Ismail and Materwala, 2019). Nearly all IoT devices have bounded storage and random access memory with 8-bit or 16-bit microcontrollers (Bosamia and Patel, 2020). Emerging technologies, such as blockchains, can be altered to accommodate IoT networks' and devices' limitations and requirements. Nowadays, blockchain has become the most secure medium of data transmission. The main goal of this paper consists of the usage of web3 storage in the fusion chain platform along with the fusion chain's lightweight block structure that can be used by IoT devices resulting in minimal CPU power consumption. Moreover, the development of two consensus algorithms for the performance evaluation of the fusion chain blockchain to balance the computational power with the Internet of Things is proposed.

1 INTRODUCTION

Blockchain's underlying technology has the potential to change how we consume information completely. As the Blockchain grows, the operating node requires significant storage, processing power, and data transparency. The ability to establish trust in remote settings without the need for authority is a technological advancement that has the potential to change several industries, including the Internet of Things. Resources are typically limited in IoT devices. The devices require much processing power and scalability to handle planned and specified computations. These devices' high power consumption is a significant drawback and performance constraint.

We believe that Blockchain will be one of the following disruptive technologies that IoT will use to surpass its current limitations, following in the foot-steps of other pioneering technologies like big data and quantum computing. In contrast to Hyperledger Fabric and Ethereum, the light block structure has been suggested for the fusion chain, as seen from the literature on block structures of different blockchain systems (Na and Park, 2021) (Thakkar et al., 2018). This paper aims to propose a blockchain topology with web3 storage. To test the performance of CPU power consumption, both the PBFT and RAFT consensus algorithm implementation is included. (Na and Park, 2021) (Yao et al., 2021).

The rest of the paper is organized as follows: Section 2 provides an overview of blockchain technology and Internet of Things (IoT) challenges. The related work is presented in Section 3. Section 4 describes about the system architecture and architecture flow. Section 5 includes the frontend and backend flow. Section 6 describes about the achieved results. Conclusion and Future Work is mentioned in Section 7.

[a] https://orcid.org/0009-0004-5795-0514
[b] https://orcid.org/0000-0002-6308-9191

Lisa, T. and Saivichit, C.
Optimized Fusion Chain with Web3 Storage.
DOI: 10.5220/0012147800003541
In *Proceedings of the 12th International Conference on Data Science, Technology and Applications (DATA 2023)*, pages 613-620
ISBN: 978-989-758-664-4; ISSN: 2184-285X

2 BLOCKCHAIN OVERVIEW AND IoT CHALLENGES

2.1 Overview of Blockchain

The roots of blockchain technology were established in the late 1980s and early 1990s (Lamport, 2019). To prove that nothing had been changed in the collection of signed copies, a signed data chain was employed in 1991 as an electronic ledger for digitally signing documents (Narayanan et al., 2016). Bitcoin is only one of many blockchain-based inventions now under development. Before Bitcoin, other, less well-known electronic payment systems existed. Because no single user could control the virtual currency and there was no single point of failure, the distribution of a blockchain-enabled Bitcoin increased its utility. As a result, direct user-to-user transactions without the involvement of third parties were made possible. The Bitcoin Blockchain allows users to maintain their anonymity, but even if users' identities are concealed, all transactions and account IDs are still viewable to the general public. In the absence of authorized intermediaries, the four fundamental characteristics of blockchain technology outlined below foster the necessary confidence within a blockchain network:

Ledger: The system keeps a complete record of all transactions in an append-only ledger.
Secure: The ability to rely on blockchain technology to safely store and verify data is ensured by sophisticated cryptography.
Distributed: Participants on the blockchain networkare transparent to each other because the ledger is distributed among them.
Decentralized: A decentralized ledger grows the number of nodes and makes a blockchain network more resistant to malicious attacks.

2.2 Categorization of Blockchain

Depending on the permission system used to determine who is allowed to maintain a blockchain network, several categories may be identified. Its four classifications are a public, private, consortium, and hybrid blockchain topology.

Publicly controlled blockchains are open, unconstrained, and available to all users. The majority of bitcoin trading and mining now takes place on public blockchains. Blockchains that have permissions owned by a single entity are called private blockchains. They are only partially decentralized because the general public can only use them to a limited extent.

A consortium blockchain is a permissioned blockchain maintained by multiple organizations rather than a single organization.

Hybrid blockchains are ledgers controlled by one organization but accessible to public blockchain inspection, which is required to verify some transactions.

2.3 Pillars of Blockchain

Blockchain technology is built upon four pillars:
Cryptography: Cryptography is a vital part of blockchain security. A blockchain encrypts data before transferring it to a destination using cryptography, which utilizes symmetric and asymmetric keys and hash functions (Bosamia and Patel, 2020).
Distributed Ledger: It is widely available, shared, and synchronized by agreement across many locations. The distributed ledger is decentralized and keeps track of every contract and transaction between various parties and sites (Bosamia and Patel, 2020).
Smart Contracts: Smart contracts are blockchain-stored computer programs that only launch when specific requirements are satisfied. They are used to automate contract execution and guarantee that everyone is notified of the conclusion as quickly as feasible (Salimitari et al., 2020).
Consensus Algorithms: The blockchain network's nodes reach a consensus on the distributed ledger's current state using a consensus algorithm. The primary motivation of the publishing node is unquestionably financial gain, not a concern for the welfare of other publishing nodes or the network.

2.4 Classification of Blockchain Consensus Algorithms

Depending on the working mechanism, blockchain consensus algorithms are classified into two categories: Proof-Based and Voting-Based, which is shown in Figure 1. Further, the Voting-Based algorithms are divided into two classes: Crash Fault Tolerant and Byzantine Fault Tolerant. Among these two, PBFT (Practical Byzantine Fault Tolerance Consensus Algorithm) and RAFT (It is not quite an acronym but named after Reliable, Replicated, Redundant, And Fault-Tolerant) are proven suitable for the Internet of Things. Since all IoT networks desire high throughput, low latency, and minimal computational overhead, the PBFT and RAFT are preferred among most consensus algorithms. They can operate normally even when more than one-third of all nodes engage in malicious behavior.

Fast throughput and low latency are all benefits of PBFT that make it a good choice for IoT networks. In RAFT, where as much functionality as possible is concentrated on the leader, and leader election is necessary as part of the consensus process (Salimitari et al., 2020). PBFT may work adequately in the presence of up to one-third of all nodes engaged in malicious activity. As far as we know, RAFT is the only consensus-based log replication method that supports fewer message types.

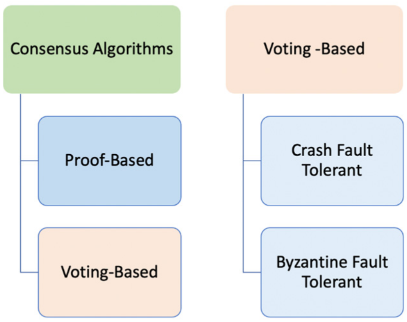

Figure 1: Classification of Blockchain Consensus Algorithms.

2.5 An Overview of IoT Architecture

An IoT architecture is a four-step procedure whereby data is collected by sensors and sent to the corporate data center for processing, analysis, and storage. The first step of the procedure entails using sensors and actuators to keep an eye on and control a physical process or phenomenon (Na and Park, 2021). The second step consists of internet gateways and data-gathering tools. Pre-processing reduces the digital data entering the data center or cloud in the third stage. The final step involves a thorough analysis in the data center or cloud, where a decision is made after carefully analyzing the data for business requirements (Yao et al., 2021).

2.6 IoT Device Classification

IoT devices fall into one of two categories:
Non-Constrained Devices: These devices have a direct Internet connection capability (Ahmed and Shilpi, 2018). An example is an Internet of Things device connected to an automobile through a Mobile Network Operator. Another example is a wearable device that sends a patient's health data to a distant server.

Constrained Devices: Constrained devices are those that have limited memory and processing speed. Typically, they cannot access the Internet due to an external barrier (Ahmed and Shilpi, 2018).

2.7 Challenges to Adopt Blockchain in IoT

The following difficulties exist when utilizing Blockchain on IoT devices:
Computation: The cost of blockchain activity is too high for small-scale IoT devices. The demand that a full node in the Blockchain validates and searches every block and transaction may be a significant load for IoT devices with limited resources. IoT devices are incompatible with consensus techniques like PoW. As a result, IoT devices cannot supply sufficient CPU power for PoW operations.
Storage: The entire Bitcoin Blockchain is about 150 gigabytes, and the Ethereum Blockchain is almost 400 gigabytes (Vujičić et al., 2018). So, IoT devices can not afford the extensive storage that Blockchain requires. In the past nine years, Bitcoin has received about 5105 additional blocks.
Communication: Blockchain, a peer-to-peer network continuously exchanging data, must maintain consistent records, including the most recent transactions and blocks. Wireless communication methods, often used to link IoT devices, are less reliable than traditional connections in typical Blockchain applications because of shadowing, fading, and interference. Blockchain requires much more processing power than wireless technologies do.
Energy: A single battery charge can power some IoT devices for extended periods. However, blockchain-related activities necessitate a lot of communication and energy-guzzling computers. As a result, IoT devices cannot support Blockchain (Lee et al., 2007).
IoT Device Mobility and Partition: Blockchain performance may suffer due to IoT device mobility. Device mobility in a wireless network with infrastructure support may increase the amount of signaling and control messages sent. On the other hand, network partitioning separates wireless ad hoc networks into units when mobile nodes move along different paths.
Latency and Capacity: Excessive latency is used in decentralized Blockchain networks to guarantee consistency. The latency that Blockchain frequently tolerates is a concern for many IoT applications.

3 RELATED WORK

3.1 Fusion Chain

A key objective of FUSION is to develop a platform level public chain in the crypto-finance era that connects all values, conducts thorough financial operations, interacts with a wide range of communities and tokens, and links centralized and decentralized organizations to expedite the Internet of Values' commercialization. Using distributed nodes, FUSION will build a public chain that can map other blockchain tokens to it and support cross-chain smart contracts by storing the private keys of many tokens on it. As well as improving the scalability and interoperability of the current Internet of Values, it will establish itself as a comprehensive crypto financial platform:

- By supplying their private keys to the distributed nodes of FUSION, tokens are interoperably mapped to the FUSION public.
- Putting these off-chain assets and data under the control of centralized institutions enhances scalability. As a result, blockchain-based smart contracts can interact with data and physical assets.
- The performance of FUSION needs to be improved to handle a large number of tokens by fully utilizing distributed nodes to perform distributed parallel computing.

Fusion Chain's purpose is to leverage blockchain technology in order to provide an IoT-compatible platform by providing a lightweight block structure, InterPlanetary File System(IPFS), and IoT-friendly PBFT consensus algorithm. However, the IPFS of the fusion chain consumes a lot of bandwidth and offers limited storage.

3.1.1 Block Structure Affects Storage Overheadand Power Consumption

In the blockchain, a block contains some data fields. The number of data fields inside data fields varies depending on the blockchain platform design. In comparison with other blockchain platforms, such as Hyperledger and Ethereum, the fusion chain offers the lightest block structure. The fewer data fields a block will have in it, the calculation performed to reach the consensus will become easier. This is how it will reduce the storage overhead and thus gets less CPU computational power. Figure 2 shows how the block structure affects the power consumption.

3.2 Web3 Storage

Web3 storage is a decentralized platform of services and APIs that comes with blockchain technology. It is built on top of IPFS and Filecoin. It stores data in a distributed manner on a network of multiple nodes. It uses identity protocols like IPFS and Filecoin to store data. Moreover, these protocols provide information

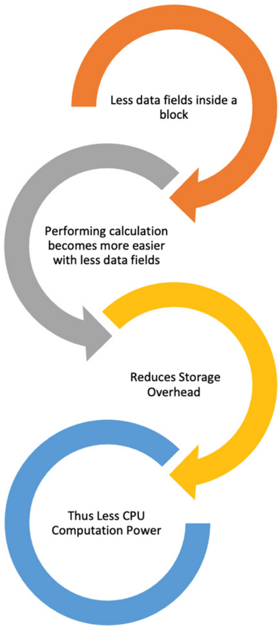

Figure 2: How the Block Structure Affects the Power Consumption.

about the storage destination of the data and the recovery process of it using its unique Content ID. In order to interact with its service, it provides some web user interface, client library, and URL.

It is trustworthy because all is in cryptography. Content addressing and Filecoin proofs play a prominent role here. It computes CIDs (Content Identifiers) locally before uploading the data and retrieving the data CIDs are validated locally. The data is safe in Filecoin; the user can check the Filecoin blockchain at any point to confirm. Users can pull the data down via IPFS once it is on the network. Thus it provides redundancy by storing the data on several IPFS nodes. Filecoin webstorage token I'd creates instance for storing the data. Then loT device data is sent to Filecoin, and Content ID (CID) from Filecoin is stored in blockchain. Figure 3 shows filecoin system.

4 ARCHITECTURE

This section describes the system architecture. The system architecture and the architecture flow diagrams are depicted in Figure 4 and Figure 5, respectively.

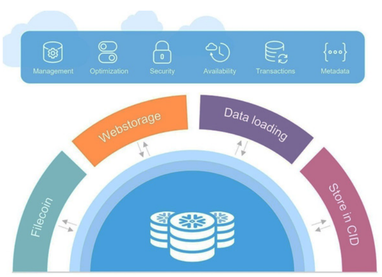

Figure 3: Filecoin System:Global Services.

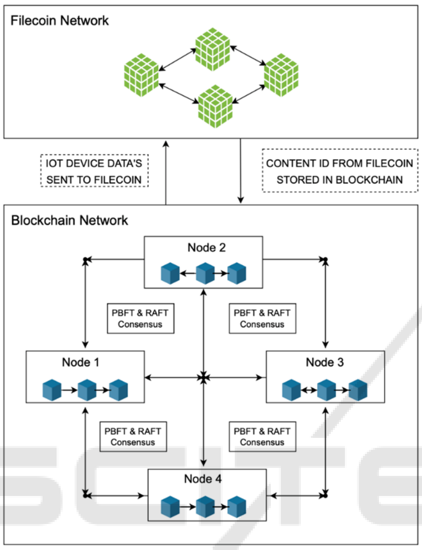

Figure 4: System Architecture.

Filecoin web storage is used as the storage system, and the token ID is generated wherein we create an instance for storing the data. So, we have a connection among the Filecoin, IPFS, and that instance within our node. When the new devices are added, a structured json is created, and these json data will be passed to the web storage that generates transactions. Then the loT device data is sent to filecoin, and Content ID (CID) from filecoin is stored in blockchain. The IPFS storage will return CID, that's nothing but a hash value based on the file properties. On storing the data, IPFS will return the hash to retrieve the data from CID. These act as the API to get data from filecoin from the web3 storage.

PBFT and RAFT Consensus algorithms are applied to eliminate the malicious faulty nodes preventing unauthorized nodes from validating bad transactions in the blockchain network, thus enhancing security. Figure 6 shows IPFS and Filecoin Instance connection along with PBFT and RAFT.

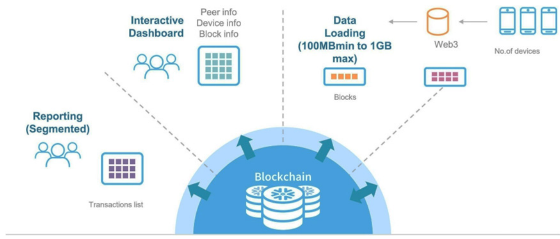

Figure 5: Architecture Flow Diagram.

5 IMPLEMENTATION

This section contains information about the implementation, which includes the frontend flow and backend flow.

The fusion chain API has been re-written in the implemented system, which is imported the opensource fusion chain API (package.json in the code) and re-written in the node.js backend by modifying the json file to improvise the PBFT and RAFT by setting it as the source package denoting as iotblockchain-pbft-raft. It acts as the backend API URL as /infusion. The code is written in such a way by remapping the integrity and configuring the dependency file with SHA-512 algorithm that reduces computational power by enhancing the transaction speed to get it stored in the blockchain. The screenshots of the code implementation and the json data are shown in Figure 7.

The process flow starts from the blockchain network, which has individual nodes that represent the IoT devices. When the IoT application is executed, the backend API provides data to the frontend through a port of peer-to-peer connection. The nodes exhibit peer-to-peer connection communicating with each other, which is collectively within a blockchain network. It denotes home automation control data connecting each other that has to be stored in blockchain, which creates transactions. Thus, performing the transactions on blockchain also displays the number of nodes connected in the frontend through the web socket.

Once the transaction has taken place, PBFT pre-prepares announcing to all connected nodes that a new transaction has been created to commit and validate the signature from where it has been received by verifying the transaction so that the successful transactions are ready to get added in the blockchain. Once all the nodes are validated by the PBFT Consensus method, all the successful transactions will be added to the blockchain eliminating the malicious nodes.

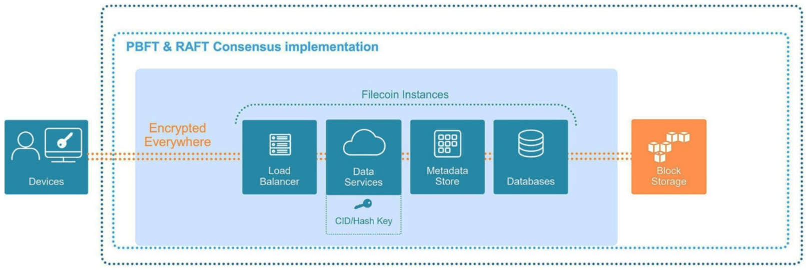

Figure 6: IPFS and Filecoin Instance connection.

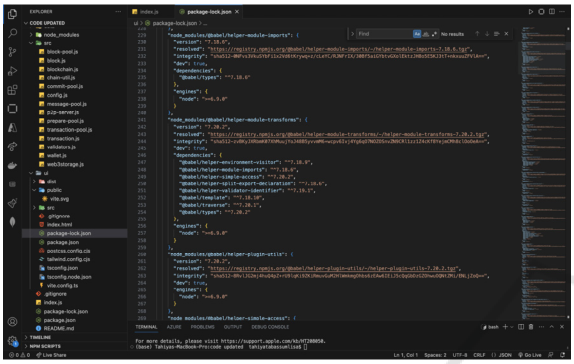

Figure 7: Configuring the Dependency File with SHA-512 Algorithm.

After which, the IoT device data will be stored in the filecoin network passing the CID, which again stores in blockchain upon retrieval keeping all the transactions within the blockchain. The timed-out nodes are handled by the RAFT algorithm through electing the leader node by the follower node instructions based on the vote to rejoin the network. The handshake timeout is a time period in which a node should establish a connection with another node. In the peer-to-peer network handshake timeout issue will happen when the establishment fails within this period.

This implementation code can be found online[1].

6 RESULTS

This section contains the results part. The output is presented through the dashboard, and some messages about the number of peers availability have been displayed.

Our dashboard shows six sections: Devices, Metrics, Peers, Transactions, Blocks, and Comparision in Figure 8.

[1] https://github.com/61714100/Optimized-FusionChain-with-Web3-Storage

In the Devices section, we can add a new device to the home automation system, and then it will be added to the dashboard and metrics. Here, we can also choose the device power level and device name. The addition of a new device is presented in Figure 9.

In the Metrics section, we can see the exact information about the time and date of adding the device. Moreover, it shows the turn-off time and usage of the device as a graph. All these pieces of information are shown in Figure 10 shows those information.

The Peers section displays the average CPU usage, current CPU usage, and current RAM usage for the running node. Figure 11 shows those information. The Transaction section shows the list of transactions. When a new device will be added, it will have a new transaction added. In Figure 12, we can observe the blocks list, and then previously added and verified transactions will be executed in the transaction displaying the list of transactions.

The Blocks section shows the chain of blocks added to the blockchain. When a transaction is made, and the transaction reaches its threshold, a new block will be added to the chain. The list of blocks will also be displayed then. In Figure 13, we can observe it.

In Figure 16, we can see the transaction and block has been added to the console.

Say, for example, it might have four transactions and four blocks with two peers mostly, it’s using 100 MB min and even 1GB max till 1.4 percent that displays metrics transaction comparison between devices. This is the result example, the output that we get when the code is executed.

The CPU and memory consumption is reduced to 1 percent and 3 percent, respectively. The CPU utilization is reduced due to the implementation of a lightweight block structure of fusion chain supporting IoT devices through an optimized filecoin system. The storage size is reduced due to the IPFS implementation that decentralizes content storage through CID to store data in the form of the hash value to the blocks in the blockchain network.

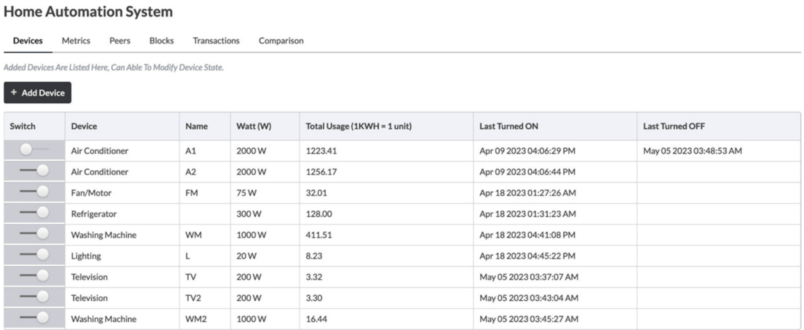

Figure 8: Dashboard.

The datasets aren't a specific approach, but latency time for loading data to IPFS, processor information such as time taken, and storage utility can be used as data to compare the system performance. The current system utilizes minimal transactions and blocks creation using 100MB min to 1GB max.

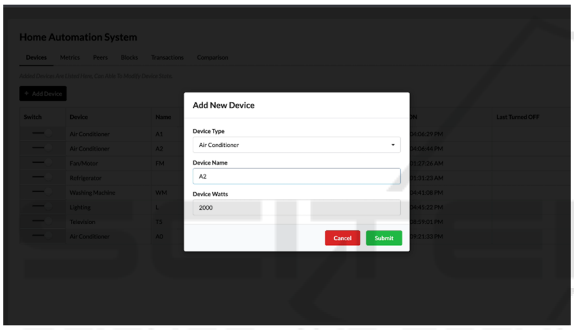

Figure 9: Adding New Device.

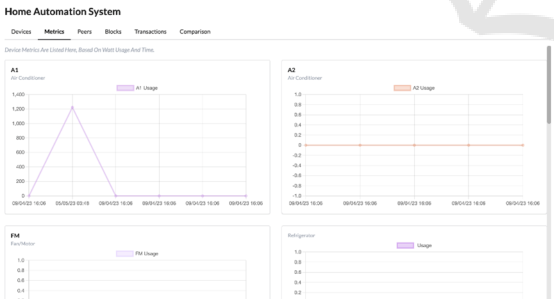

Figure 10: Device Usage Information.

We have executed the code in the M1 processor Macbook Pro which has a RAM (Random Access Memory) of 8 GB. Only two nodes could be run at a time in this local machine. Moreover, it does not show fluctuating percentage differences respective of the devices as the loading data is in Kilobytes. In order to add more nodes to the system and work with big-size data, it will need a high-processor machine with extended RAM. Moreover, this application is executable both in Windows and Linux operating systems.

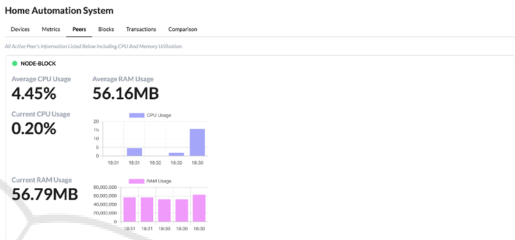

Figure 11: Average CPU usage, Current CPU usage, and Current RAM usage for Node.

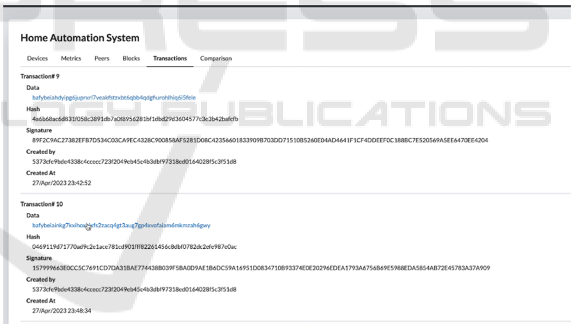

Figure 12: Transaction Added in User Interface or Front end.

7 CONCLUSION AND FUTURE WORK

The design and implementation of the core idea of a fusion chain blockchain with better storage is implemented in this study. This work integrated web3 storage as improved storage from earlier work to decrease power consumption and improve storage quality (Na and Park, 2021). As for IoT devices, a home automation system has been used to test the performance of the work using the PBFT and RAFT consensus algorithms. The proposed system execution results in reduced CPU and memory consumption to 1 percent and 3 percent respectively, having the size of the blockchain reduced that uses 100MB min to max 1GB for loading data with minimal transactions and blocks.

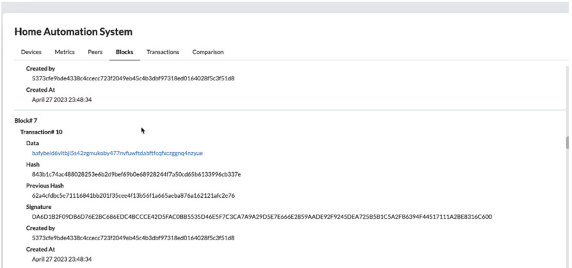

Figure 13: Block Added in User Interface or Front end.

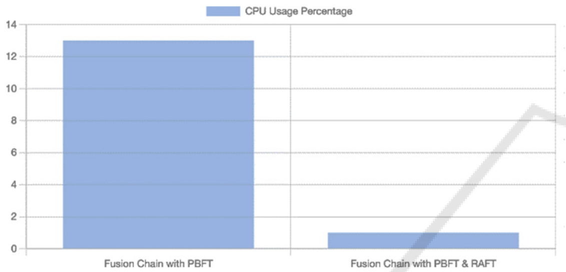

Figure 14: CPU Consumption Comparison: Fusion chain using PBFT using 13% of CPU with four nodes. In the new solution, code was optimized using the new concurrency model CPU usage was reduced to 1%.

This project indicates a clear path toward the implementation of the web3 storage, PBFT, and RAFT inside the fusion chain platform's internal system architecture. Moreover, connecting real time IOT devices like raspberry pi to merge with the blockchain platform in order to analyze the performance with real life implementation.

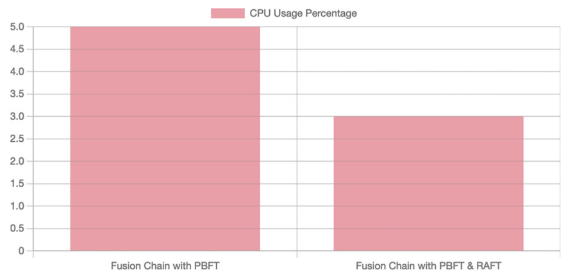

Figure 15: Memory Consumption Comparison: Fusion chain using PBFT using 5 MB of memory with four nodes. In the new solution code, it used 3 MB as we included RAFT it required new memory to process.

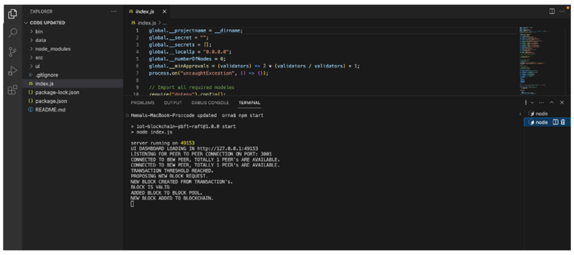

Figure 16: New Transaction and Block Added in Console.

REFERENCES

Ahmed, I. and Shilpi, M. A. (2018). Blockchain technology a literature survey. *Int. Res. J. Eng. Technol.*, 5(10):1490–1493.

Bosamia, M. and Patel, D. (2020). Comparisons of blockchain based consensus algorithms for security aspects. *Int. J. Emerg. Technol.*, 11(3):427–434.

Ismail, L. and Materwala, H. (2019). A review of blockchain architecture and consensus protocols: Use cases, challenges, and solutions. *Symmetry*, 11(10):1198.

Lamport, L. (2019). The part-time parliament. *In Concurrency: the Works of Leslie Lamport*, pages 277–317. Lee, J.-S., Su, Y.-W., and Shen, C.-C. (2007). A comparative study of wireless protocols: Bluetooth, uwb, zig-bee, and wi-fi. In *IECON 2007-33rd Annual Conference of the IEEE Industrial Electronics Society*, pages 46–51. Ieee.

Na, D. and Park, S. (2021). Fusion chain: a decentralized lightweight blockchain for iot security and privacy. *Electronics*, 10(4):391.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S. (2016). *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press.

Salimitari, M., Chatterjee, M., and Fallah, Y. P. (2020). A survey on consensus methods in blockchain for resource-constrained iot networks. *Internet of Things*, 11:100212.

Thakkar, P., Nathan, S., and Viswanathan, B. (2018). Performance benchmarking and optimizing hyperledger fabric blockchain platform. In *2018 IEEE 26th international symposium on modeling, analysis, and simulation of computer and telecommunication systems (MASCOTS)*, pages 264–276. IEEE.

Vujičić, D., Jagodić, D., and Ranđić, S. (2018). Blockchain technology, bitcoin, and ethereum: A brief overview. In *2018 17th international symposium infoteh-jahorina (infoteh),* pages 1–6. IEEE.

Yao, W., Ye, J., Murimi, R., and Wang, G. (2021). A survey on consortium blockchain consensus mechanisms. *arXiv preprint arXiv*:2102.12058.