ISSN: 2182-2069 / E-ISSN: 2182-2077

Securing Cloud Data Storage through Blockchain-Enhanced Encryption

Firas Abdulrahman Yousif[1*], and Mariam Raheem Mirza[2]

[1*]Department of Computer Science, Faculty of Education, University of Al- Hamdaniya, Ninavah, Iraq. firasabdulrahman@uohamdaniya.edu.iq, https://orcid.org/0000-0002-3259-5577

[2]Department of Computer Science, Faculty of Education, University of Al- Hamdaniya, Ninavah, Iraq. mariam.mirza@uohamdaniya.edu.iq, https://orcid.org/0009-0006-2957-5731

Received: November 20, 2024; Revised: December 28, 2024; Accepted: January 17, 2025; Published: February 28, 2025

Abstract

Blockchain technology has brought a new change in many sectors mainly through provision of decentralized transactional solutions and it is an open, continuously growing list of records, which is distributed and not controlled by centralized authorities. The current regulation is the first one of such kind because it encompasses payment, communication, registration, and monitoring of transactions between members, without the need to have a central authority to manage the needs of the organization. There are however, challenges, which persist for example in data storage and scalability. This paper presents SetChain, a new solution that in order to eliminate these problems defines structured epochs for data storage and transaction grouping. This best suit the arrangement of storage as it retains the history of transactions. SetChain also uses the transaction signatures to ensure the authenticity of the data being used for the chain, upping security and trust. It applies consensus mechanisms to mitigate such activities and guarantee the system's dependability. As for the seen in our simulations on the decentralized network wherein 20 nodes were used, the transactional throughput varied greatly, and this started from 440 to 520 by node. During the testing of the transaction validation with a sample of one thousand transactions out of the ten thousand total number deemed valid, forty-three hundred and five hundred and thirty-four were valid and the invalid ones were mainly due to failure in balance limitations. In addition, other transaction performance patterns beside node balance were derived from data storage simulations with the help of pandas. Another emergent attribute was the dealing of the Byzantine faults in the framework, and the entire network was sustained. It reveals highly improved means of storing the data of a blockchain networking than before, scalability and security and proposes a viable model for future decentralization agendas.

Keywords: Scalability, Data Storage, SetChain, Blockchain (BC), Cloud Computing.

1 Introduction

Cloud computing as we can define now is a global stage where users are provided with the means to store and shared data with remote parties securely (Sunyaev & Sunyaev, 2020). This user- centric solution is highly favored, as it eliminates issues to do with transfer of data between the two regions without any delays or interruption. Accordingly, personal storage space for each user is provided, and

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 1 (February), pp. 130-152. DOI: *10.58346/JISIS.2025.I1.009*

*Corresponding author: Department of Computer Science, Faculty of Education, University of Al- Hamdaniya, Ninavah, Iraq.

data storage and transfers can be completed virtually on-demand from distant servers (Yu et al., 2021; Devaraj et al., 2020).

In addition, cloud computing is not limited to store data in the cloud but also includes the capacity to process information as per the commands which the user feeds into the servers through cloud (Clementine et al, 2014; Idowu & Eiriemiokhale, 2020). Thus, the main benefits of using cloud computing are availability, data security, versatility, and easy organization of servers. The attractiveness of these benefits has led to a substantial surge in the adoption of cloud computing in recent years. Nonetheless, the prominence of cloud computing has also drawn attention to its privacy and security challenges during data transmission. The act of storing data in cloud servers invariably creates questions related to protection of data in question. Data privacy is especially important for cloud computing, as data owners cannot have the same level of information about server-side difficulties they may face (Krishnaraj et al., 2021; Premkamal et al., 2021). The server-side challenges they might encounter (Krishnaraj et al., 2021; Premkamal et al., 2021). This fact clearly highlights the significance of the proper implementation of security features in cloud computing for the purpose of transfer of data through this uncomplex platform.

As a critical imperative, enhancing information security within cloud, computing is vital, especially when transmitting data across networks (He & He, 2020).

The cybersecurity landscape has been impacted by factors such as outdated devices, devices with limited memory, and hasty password changes that occur without a comprehensive understanding of their potential consequences. These factors have contributed to the widening scope of cybersecurity vulnerabilities, escalating the risks associated with the transmission of sensitive data through cloud infrastructure (Lakshmi et al., 2021).

In recent years, the increasing threat of cyberattacks has exposed the vulnerabilities of Internet of Things (IoT) devices, which are particularly prone to breaches due to insufficient security measures (Campos et al., 2022). While recent attempts have been made to discuss security challenges in IoT, proper guidelines, which can help to manage the potential risks, have not been adopted yet, and hackers have attacked IoT devices as well as corporate workstations using the phishing method (Bandari, 2023; Alawida et al., 2022). In response to these threats, there must be synergy between security specialists and device creators to build effective security solutions (Safkhani et al., 2021). To mitigate the control and trust concerns in traditional and current cloud contexts, the identity of blockchain (BC) technology that implement decentralized ledgers to safely store transactions has emerged (Xu et al., 2020; Wei et al., 2020; Rejeb et al., 2022). Invented for Bitcoin in 2009, blockchain has advanced to accommodate innovations next to smart contracts that improve its transactional capabilities besides promoting the decentralised applications across several economies and for various utilities such as DeFi and Web3 (Sagheer & Dawood, 2021).

Embedded into the principles of distributed ledgers is the “blockchain” architecture. This is a series of blocks in which each block contains a list of user transactions (Haber & Reichman, 2020). The data on this ledger is maintained and checked by multiple servers and which is decentralized without having worth keeping of the key, because of the powerful algorithms that cannot be manipulated maliciously. However, the ability to scale still presents a problem for use of blockchain technology (Cheng & Wei, 2024). The requirement for consensus algorithms that can guarantee the decentralised system’s security and reliability can lead to times of slowness (Velliangiri, 2024). For example, Ethereum, a superior blockchain technology, validates below four blocks per minute, often containing below two thousand transactions per a single block. Compared to Visa, MasterCard and PayPal, bitcoin’s number of transactions is even lower. Some of such limitations negatively affect the efficiency required by several

decentralized applications, which could slow down further adoption. Furthermore, such restricted throughput can increase the cost of each operation since the demand is high due to its restriction. As more firms eyed on blockchain technology, there is an increase in approaches seeking to improved scalability of the technology. Among these strategies are:

- Developing faster consensus mechanisms.
- Implementing parallelism, with techniques such as sharding.
- Constructing niche blockchains designed for specific applications that can communicate between chains (Nihlani & Chhabda, 2024).
- Exploring the"layer 2" (L2) approach, where certain functions are taken off the primary blockchain but retain security benefits (Said et al., 2024). Examples of L2 solutions include off-chain computation of Zero-Knowledge, proofs that are subsequently verified on-chain, the introduction of channels like the Lightning network, or the use of optimistic rollups, which minimize the need to run contracts on servers unless required for claims or dispute resolution.

In our study, we introduce a unique angle to improve blockchain scalability, hinged on an intriguing observation. While traditionally it is believed that for cryptocurrencies to prevent double spending, there needs to be a complete order of transactions, we have identified that several applications, even some cryptocurrencies, can function effectively with partial ordering. Our proposed solution is a Byzantine-fault resistant model of a continually expanding distributed set, enhanced with a synchronization mechanism to ensure consensus across servers at specific checkpoints. During the periods between these checkpoints, there might be some lag in the uniformity of data knowledge across servers.

We have dubbed this novel distributed structure "setchain". When a blockchain incorporates Setchain, it can synchronize block consolidations with these barrier synchronizations, yielding an efficient set datatype that is side by side with the main blockchain. This system maintains the robust Byzantine-resistant qualities of the original blockchain.

SetChain's development is driven by its potential in various applications:

- Mempool Logging: Currently, user transaction requests are held in a mempool before miners select them. Once these are mined, the initial data disappears. To chronicle and analyze the mempool's progression, there is a need for a supplementary system that can efficiently log all mempool interactions without hampering the primary blockchain's operations. Setchain, when utilized as an auxiliary chain, presents itself as an apt solution for creating such a trustworthy logging system.
- Enhancing Scalability with L2 Optimistic Rollups: Plat- forms like Arbitrum employ optimistic rollups, leveraging the idea that computations can be performed off-chain, relegating only the claim summaries to on-chain operations. In this setup, users suggest the subsequent state for the "contract". After a designated period, the on-chain arbiter smart contract accepts a proposed move as valid and implements the designated changes. If conflicts arise, they are managed on-chain through a resolution mechanism (Al-Barazanchi et al., 2022). Such a framework does not demand a rigid transaction order—just a record of proposed actions. Furthermore, the process of resolving conflicts can be streamlined to merely validating claims, a task which Setchain maintainers can potentially oversee (Qalati et al., 2022).
- Sidechain for Data Management: Setchain can also serve as a foundational side-chain platform that facilitates data storage and modification synchronized with the main blocks. For apps that primarily need to refresh information stored within a smart contract's space, like online ledgers, Setchain offers a quicker and cost-effective method (Yusoff & Abd Ali, 2024). This method allows

data manipulation without having to invoke the resource-intensive operations usually associated with blockchains.

In our study, the proposed diagram of the setchain, Figure 1 illustrates the workflow and data management within a decentralized network (Mızrak, 2023). The user initiates the process, represented at the bottom of the diagram, where data flow originates. This data is then processed through cloud services, depicted as a layered stack of servers encompassed by a cloud symbol, indicating the distributed nature of the infrastructure. From the cloud services, the data is moved to a secure storage solution, as shown by the arrow leading to the 'Data Storage' icon.

The 'Data Owner' stands adjacent to the data storage, signifying control and monitoring of the data, with an emphasis on the security measures in place, represented by the connecting arrow labeled 'security'. This security is an integral part of the data's journey to the setchain (Uvarajan, 2024).

The setchain itself is represented with blocks interconnected with each other as a downward link, referencing the traditional blockchain representation but still tailored to the setchain. All the blocks inside this network are painted in color, which hints about the types of the transactions or data points treated within the setchain system. This is the last stage of the data journey, during which it is safely preserved, as well as verified and protected by utilizing essential attributes of setchain technology, namely decentralization, security, and data integrity (Salman et al., 2023). Our contributions in this research are:

- Introduction of Set Chain: A novel framework to address data storage and scalability challenges in blockchain networks.
- Structured Epochs for Data Storage: An innovative method for efficient transaction categorization and storage.
- Enhancement of Security: Integrating transaction signatures to ensure authenticity and enhance network security.
- Integration of Consensus Mechanisms: Incorporating various mechanisms to improve reliability and protect against malicious activities.
- Empirical Validation through Simulation: Conducting simulations to test Set Chain's functionality and efficiency in a decentralized network.
- Comparative Analysis with Traditional Technologies: Providing a detailed comparison of Set Chain against existing blockchain technologies.

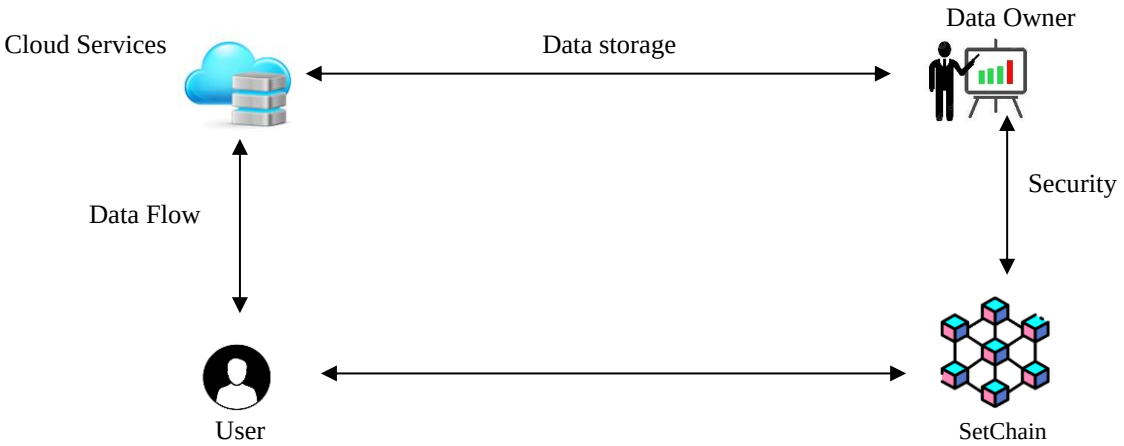


Figure 1: The Proposed Block Diagram

2 Related Work

Blockchain (BC) originated as an innovative peer-to-peer payment system that allows users to transact directly, using a public ledger where individual nodes store all the current transaction information. However, issues such as network traffic, high cost of transactions, and giving priority to transactions with high charges make scalability to be a challenge. For instance, manufacturing systems involve high levels of transacting through smart technologies, thus demanding high levels of throughput (Dedeoglu et al., 2020). For instance, to achieve an effective traceability solution, IKEA requires 7840 transactions per second, which might require partitioning the event processing over sections of the subsystem (Sund et al., 2020). Although more than 90% of companies operate as SMEs in the developing countries, their totality of throughput demands may be as high as or more than that of the large companies. For BC-based manufacturing, it is important to keep the system scalable to perform optimally even if there will always be delayed transaction processing (Abdullah, 2023). Improvements in scalabilities can be grouped into first-layer solutions which include improvements on block structures, and consensus algorithms, and second-layer solutions (L2) which offloads transaction processing from the BC network (Hafid et al., 2020). L2 solutions such as payment channels enable off chain transactions that are only.gamma, recorded on the main BC. Moreover, Taxa (Reimer et al., 2022) address scalability issue in that trustworthy hardware deals with smart contract computation while consensus remains on public blockchain. Wu et al., (2022) proposed a twin-blockchain supporting framework, which increases data security and flexibility of smart contracts and achieves high request throughput. Furthermore, Wang et al., (2020), proposed extending smart contracts with a trustable, incentive-based oracle solution to provide accuracy and probe external data. However, it implies a trade-off between scalability, decentralization, and security to think about the applications to be built.

A number of researchers have posited that blockchain technology can be applied to implementing secure data sharing models, and these models have been implemented to different degrees of efficacy and constraint. Faruk et al., (2021) proposed blockchain for sharing sensitive information using cryptographic approaches and asymmetric encryption but did not include a supervisory mechanism, and once data is shared, the owner has no say. Al Mamun et al., (2021) has offered a decentralized system to share EMRs through asymmetric encryption but it cannot prevent from exposing data to unexpected malicious personnel. In IoT context, Wang et al., (2023) created a blockchain-based solution for personal data protection employing ABE and CLE with shorter processing times, yet, PK encryption presented obvious computation overhead unfit for constrained IoT gadgets. Goyat et al., (2020) mitigated blockchain data storage problems using IPFS where data is encrypted, and access is done using private keys, but the insecurity of the unsophisticated access policy, and under-utilized consensus algorithm exposed data to dangerous nodes able to access unauthorized data (Pozi & Omar, 2020).

Most of the real-world blockchains, like that of Bitcoin and Ethereum, use a single, linear chain of blocks for maintaining and verifying transactions (Prusty, (2017). Despite the created immutable, decentralized and secure environment with this architecture there are significant issues to be concerned with in terms of scalability and data handling. For instance, Ethereum processes less than four blocks per minute, with each block, which can accommodate a small number of transactions (Oliva et al., 2020). This has a major drawback of causing congestion in the network, as transaction volumes rise, significantly higher latencies, and highly inflated gas fees rendering the system relatively inefficient for real time use. Likewise, the technical infrastructure of Bitcoin has increased these challenges because of its operation based on the Proof of Work (PoW) consensus mechanism (Oyinloye et al., 2021), which is then power-hungry and imposes time limitations to perform a new validation rate of transactions to be included in the blockchain (Velmurugan et al., 2023; Haque et al., 2024).

To address these limitations, SetChain has a more optimal and convention across the chain solution that can be actualized by employing the use of structured epochs. Different from the usual sequential pattern, the structured epochs are time lock points within which data from transactions are pulled, made coherent and stored as a coordinated whole that is easily accessible without repetitions. It reduces cycles of confirmation hence conserving resources in the process. In addition, the SetChain function proposed during the validation phase involves a method of categorizing the given transactions into the valid and the invalid ones. By decoupling validation and delegating priorities of computational processing to SetChain, the general network performance and its potential scaling capabilities are improved while never compromising the decentralization or data integrity.

From the provided related work, several knowledge gaps can be identified that can lead to potential research opportunities or areas for improvement:

- Transaction Costs and Prioritization: When networks become congested, transaction costs rise, and miners prioritize transactions with higher fees. While this is mentioned as a factor, there is no deep exploration of mechanisms to reduce congestion or ensure equitable transaction processing, especially for smaller, yet equally vital transactions.
- Scalability in Large Corporations: While the throughput prerequisites for large corporations like IKEA have been studied, it is unclear if current BC technology can meet these demands without compartmentalizing processes, which may introduce complexities and inefficiencies.
- Throughput in SMEs: The majority of businesses in developing nations are SMEs. Even though individually they may require lower throughput, collectively they can generate significant demands. The total transactional demands of SMEs, especially in developing nations, have not been extensively explored.
- Delays and Real-Time Decision Making: BC transaction processing delays may compromise real-time decisions in the manufacturing process. Delay is one of the concerns stated before but about these delays and possible strategies for their reduction, little has been said.
- Scalability Trade-offs: The strategies applied for achieving the scalability of BC can barely be optimal as they always come with a trade-off between decentralization, security and efficiency. Yet, many of these trades and their subtleties and consequences have not been rigorously analyzed.
- External Data Authenticity: This type of setup is less reliable due to outside data consistency and security: this is the last major issue with smart contracts. The reliability of such contracts relies solely with the accuracy of external data. However, as to the issue of how to constandy screen and verify this data, this remains a relatively open-ended area.
- Data Ownership and Control: In other words, once the data is shared, the original data owner has no more say as to who else to share that sensitive data with. This creates new opportunities but exposes the data to misuse, breach incidents, or even additional unlawful dissemination.
- Risks in Medical Data Sharing: While blockchain can be used to create a more decentralized means of sharing patient records, this paper's findings reveal that the technology has not provided solutions for unintended exposure to other malicious forms or how to reverse such a breakage.
- IoT Device Limitations: The use of public-key encryption can be very computationally expensive for most IoT devices, which have limited processing power. More effective yet less complex encryption modus operandi that the current conventional ones are required.
- Data Storage in IPFS: Utilizing IPFS for blockchain data storage is a novel approach, but the absence of a solid access policy and the underutilized consensus mechanism leaves potential security vulnerabilities.

Given these gaps, future research could delve deeper into optimizing BC scalability without extensive compartmentalization, understanding collective SME demands, ensuring real-time decision-making without BC-induced delays, developing mechanisms to ensure external data's accuracy continuously, and enhancing data ownership and control post-sharing.

Blockchain technology as shown in Figure 2, since its inception, has pioneered the decentralized transaction systems, providing an immutable ledger to ensure transparency and security across transactions. However, it grapples with inherent challenges related to data storage and scalability.

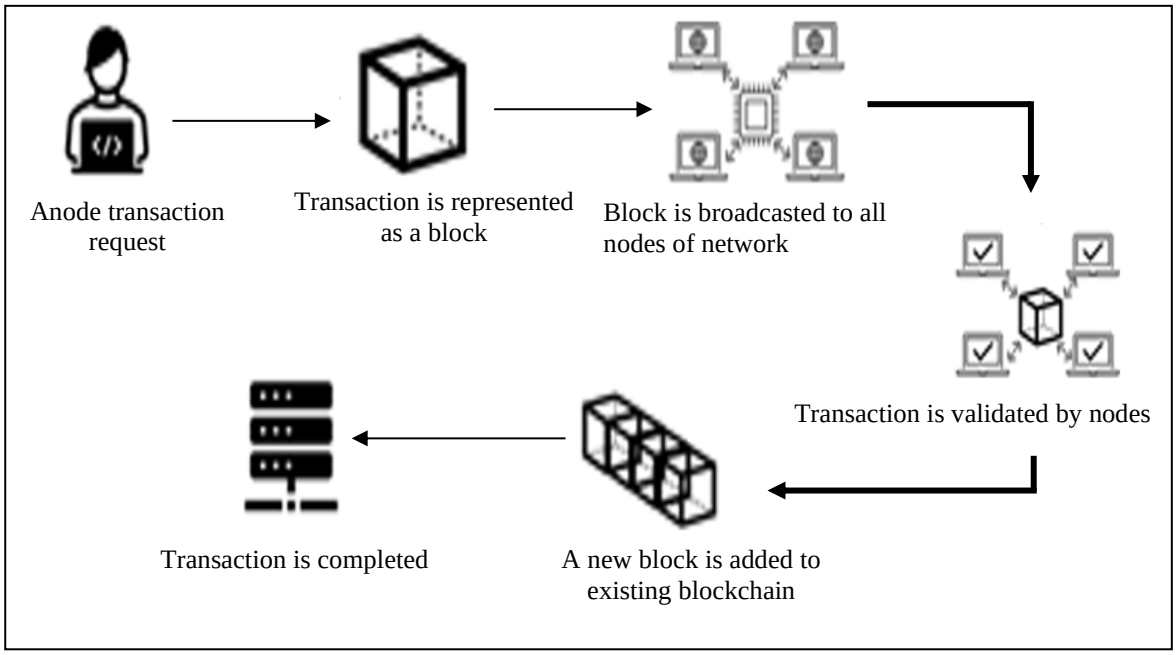


Figure 2: Traditional BC Flowchart (Yalcinkaya et al., 2020)

Table 1: Comparison Between Setchain and Blockchain Technologies

Feature	Blockchain	SetChain
Structure	Chain of blocks linked by hashes	Sets of transactions grouped into epochs
Consensus	Proof of Work/Stake	Flexible mechanisms (e.g., epochs, BFT)
Data Management	Immutable ledger	Flexible, epoch-based data management
Storage Efficiency	Linear and redundant	Optimized through structured epochs
Scalability	Limited due to single-chain structure	Enhanced by epoch-based categorization
Transaction Categorization	Not explicitly supported	Supported (valid vs. invalid transactions)
Latency	Higher due to linear verification	Lower due to efficient validation processes
Security	Hashing, digital signatures	Enhanced cryptography and epoch consensus

SetChain is a modern response specifically developed to mitigate these issues. SetChain utilizes epochs, allowing transactions to be stored in a more optimized fashion compared with traditional blockchains in which transactions are dumped linearly. This enables efficient storage while simultaneously preserving the full history of transactions. Moreover, SetChain ensures the authenticity of each transaction by utilizing transaction signatures, helping to further increase security and build trust among participants (Zhou et al., 2020). Furthermore, whereas blockchain relies on a single consensus process, SetChain is capable of adapting a variety of consensus methods, enhancing its trustworthiness and response to potential malicious activities. In conclusion, Blockchain and SetChain are both decentralized ledgers, however SetChain provides a unique way of storing and interacting with data has better security measures as well as greater flexibility in terms of the consensus mechanisms used, making it a future-oriented and flexible solution for all decentralized applications. Table1 displays a comparison table between traditional blockchain and Setchain.

2.1 Comparison with Existing Blockchain Frameworks

As illustrated in table 2 Bitcoin, Ethereum, and Layer 2 (L2) have greatly extended decentralization, security, and trust but still have insurmountable problems of improper scalability, ineffective storage, and high coefficient of delayed operations. SetChain addresses these limitations through two key innovations, systematized periods and transaction classification, all of which improve data storage and network organization. Blockchains and SetChain differ when it comes to data storage through block and transaction chains; SetChain stores data hierarchically and compressively in epochs to reduce repetition and improve scalablity. Moreover, SetChain classifies transactions at the validation stage: valid and invalid (for example), which contributes to efficient processing and reducing computational load. In addition, DAO has extensibility based on the consensus layer, in which SetChain has implemented various consensus mechanisms, such as PoW for different applications, while other blockchains are usually locked in one consensus like PoW in Bitcoin or the hybrid model in Ethereum. As opposed to Layer 2 protocols such as Optimistic Rollups, epochs in SetChain make increased scalability possible without risking data integrity as epochs are synchronized and provide accurate consensus within the network.

3 Methodology

The Method section presents out novel methodology for building and assessing the performance of the proposed SetChain framework. This comprises points from process of initial brainstorming to minute level implementation. This post will cover structured epoch design, embedding transaction sigs and consensus, and the test methodologies we used in our simulations. The flowchart in Figure 3 gives a visual representation of these steps and serves as a roadmap for our research. In every subsection below, we will explore in depth these components of SetChain, demonstrating the inner workings of SetChain, and advantages of SetChain over other solutions.

Table 2: Comparison of SetChain with Existing Blockchain Frameworks

Feature	Bitcoin	Ethereum	Layer 2 Solutions (e.g., Rollups)	SetChain
Structure	Linear chain of blocks	Linear chain with smart contracts	Off-chain computations linked to main chain	Structured epochs with transaction categorization
Consensus Mechanism	Proof of Work (PoW)	PoW (Ethereum 1.0), PoS (Ethereum 2.0)	Optimistic Rollups, ZK-Rollups	Flexible (PoW, Byzantine Fault Tolerance, etc.)
Transaction Categorization	Not supported	Not supported	Limited (mostly aggregated)	Supported (valid and invalid transactions)
Scalability	Limited (7-10 TPS)	Improved (20-30 TPS)	High scalability but off-chain	High scalability with synchronized epochs
Data Storage Efficiency	Redundant and linear	Redundant and linear	Reduced storage (off-chain)	Optimized through structured epochs
Data Consistency	Strong (on-chain only)	Strong (on-chain only)	Conditional consistency (off-chain data verified on-chain)	Strong consistency through synchronized epochs
Latency	High due to block time and PoW	Moderate depending on PoS/PoW	Low latency (off-chain operations)	Low latency with efficient transaction processing
Redundancy	High (entire chain stored on nodes)	High (entire chain stored on nodes)	Reduced redundancy (off-chain)	Reduced redundancy with epoch-based storage
Security	High (via cryptography and PoW)	High (via smart contracts and PoW/PoS)	High (security linked to main chain)	Enhanced with cryptography and consensus mechanisms
Flexibility	Low (rigid PoW and structure)	Moderate (smart contracts, PoS)	Moderate (scalability solutions)	High (modular consensus and flexible storage)
Energy Consumption	Very high due to PoW	Lower with PoS	Low (off-chain computations)	Moderate (customizable consensus mechanisms)

A. Initialization

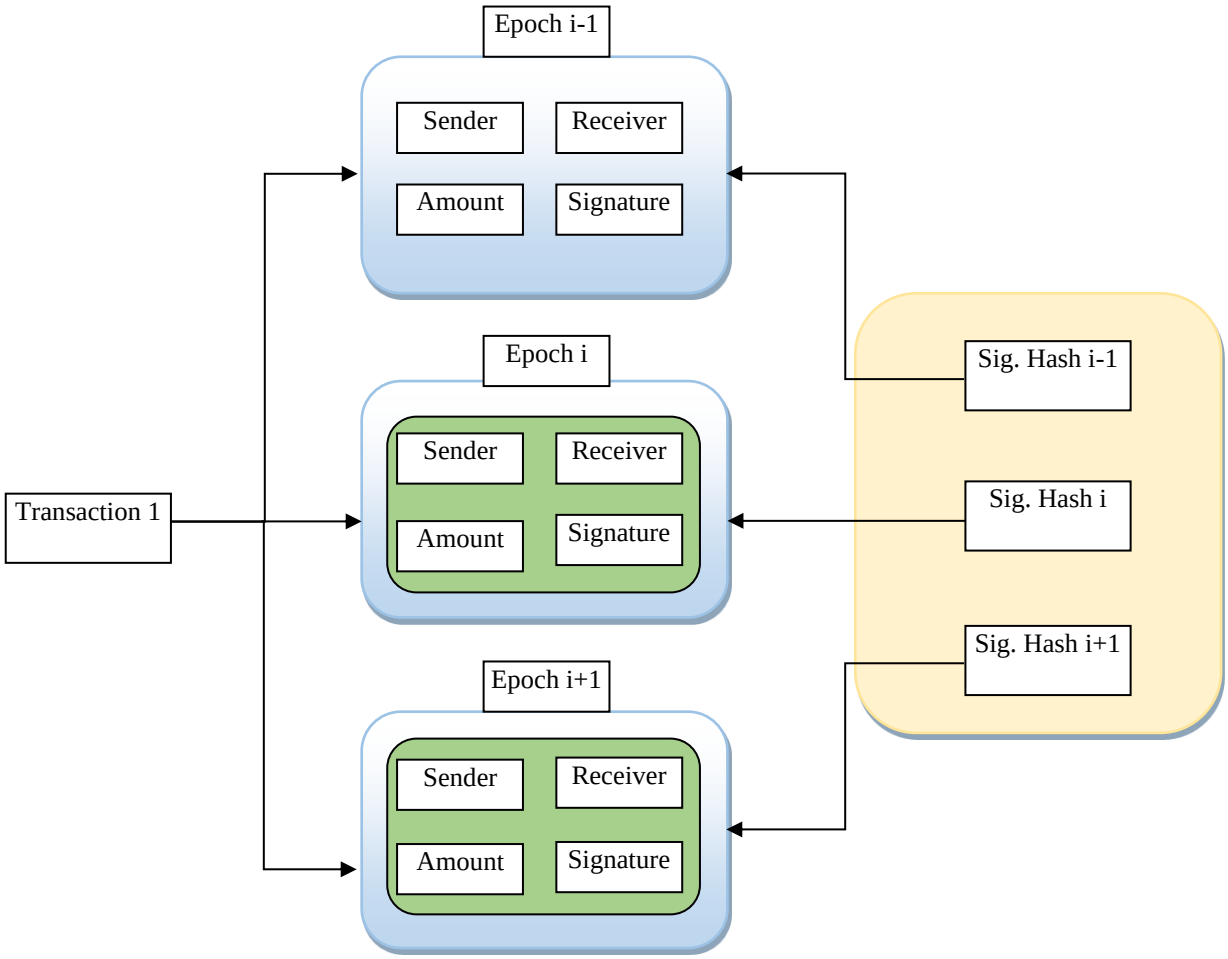
The BC simulation's initialization phase sets up all of the components that must be in place in order for the network to operate.

- Number of nodes: The BC network is made up of different actors, known as nodes. These nodes may serve multiple roles including standard users, miners, validators, etc. Then in the simulation framework, an ID identifies every node uniquely and they interact with the network by executing transactions or validating them.
- Starting Balances: Each node is given a starting balance before any activities or transactions occur within the network. This load can be uniformly spread across all nodes or assigned on some conditions or parameters. In the provided simulation framework, for instance, all nodes start with a default balance, which can be adjusted when needed.
- Other settings: A variety of parameters that help set characteristics and behaviors of a network can also be adjusted to fine-tune a simulation. These include transaction fees, choice of consensus mechanisms, block sizes, inter-block times, and many other technical details relevant to the BC being simulated.

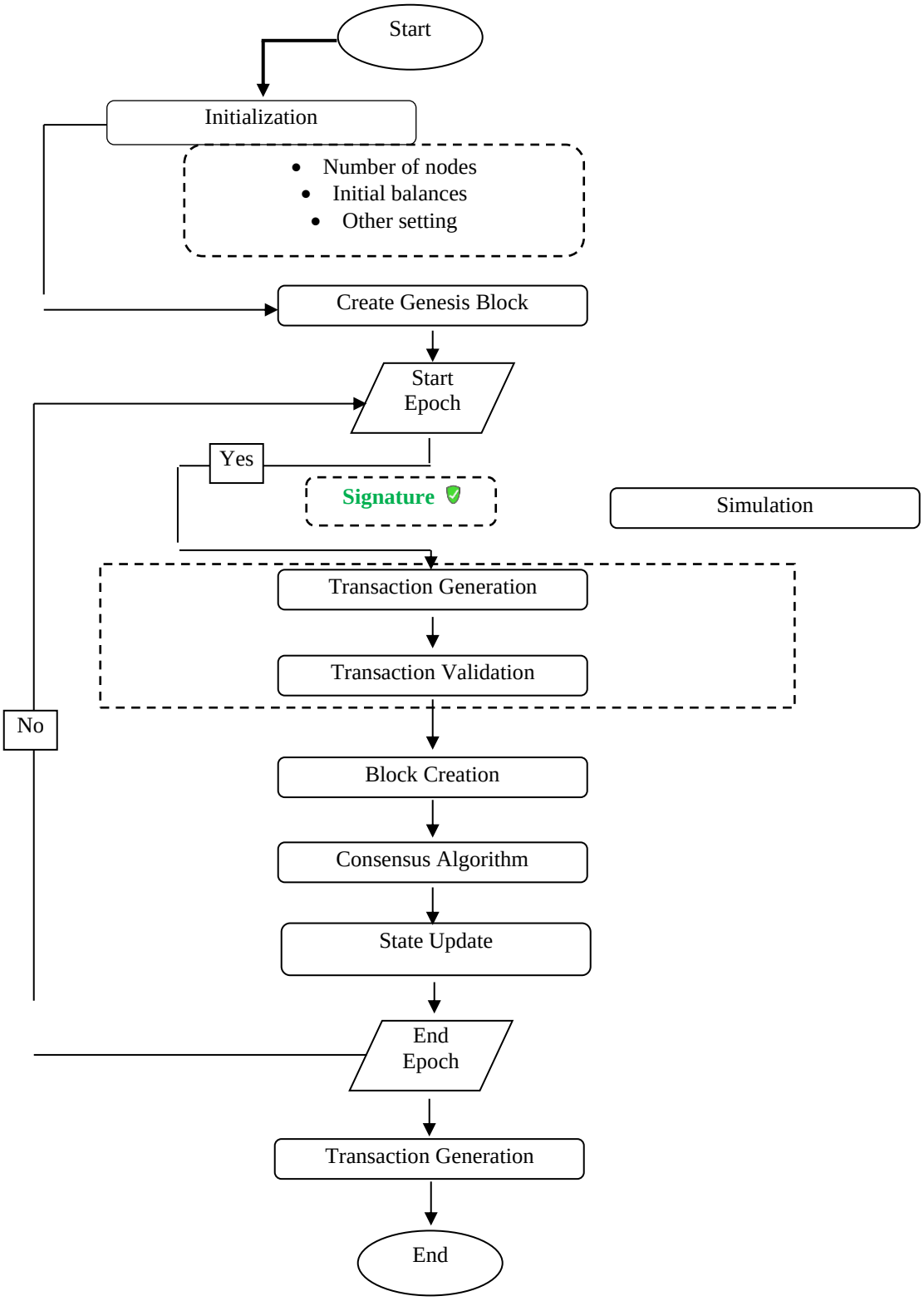
Initialization prepares the network, making it primed and ready, establishing a base for following operations (transaction generation, validation, consensus, etc.).

B. Create Genesis Block

The Genesis block, the first block in a blockchain, serves as the foundational pillar of the entire structure. Unlike subsequent blocks, it does not reference any previous blocks, marking the starting point of the blockchain. This block typically contains essential data, such as initial coin distribution, a creation timestamp, and other configuration settings, establishing key properties of the blockchain. Created through a consensus protocol, the Genesis block initiates a sequence of linked blocks that ensure immutability. Its integrity is critical, as it is copied to every node in the network, providing a verifiable and common point of origin that underpins the trustworthiness of the entire blockchain.



(a)



(b)

Figure 3: (a) Setchain Technology, (b) General Flowchart

In essence, the creation of the Genesis block is akin to laying the first stone in a building; it sets the stage for the structure that will rise atop it.

C. Simulation

The simulation phase as displayed on the algorithm 1 is more dynamic and replicates the functioning and activities of an actual BC network. This phase is cyclical and contains several steps all of which are necessary for realism and credibility of the simulation.

- Transaction Generation: This phase involves forming contracts between the nodes which may be totally random or predetermined and mimics a real life where nodes are transmitting or receiving assets or information.
- Transaction Validation: The records of transactions must be verified before being incorporated in the blockchain. This validation supports the rules of the network which include protection against double spending, checking on the digital signatures, as well as the node balances.
- Creating a Block: Confirmed transactions are bundled together and the number of transactions contained in a block may be predefined as block size and block generation rate, which may also be dynamic with respect to the simulation trials.
- Consensus Algorithm: validators some nodes contain basic functions to approve the validity of the block regarding a consensus algorithm. From the resource consuming Proof of Work to the centralized Proof of Stake or Delegated Proof of Stake, helping to maintain a single source of consensus throughout the network.
- State Update: After the consensus is achieved and the block is placed into a blockchain, the state of the network has to be modified. This includes changing the balanced and attributes of the node to cover new transactions, the symmetrical of balances among the participants.

Node corruption (Byzantine faults) can be replicated so that one can examine how the consensus mechanism performs given specific amount of adversarial activities or a technical failure. Besides, random transactions; specific transactions can be defined to examine certain situations that involve only certain nodes or transactions which have the values predetermined, thereby enabling a close study of the behaviors of the network. Simulation phase is therefore the perfect replication of a blockchain network, where stakeholders are in a position to be exposed to potential problem or scenarios in the network that may prove beneficial in real life network development.

Algorithm 1 Simulate Transactions in a Network

```
Initialize the network with 5 nodes:
network ← Network(5)
for i ← 1 to 10 do
Select a random sender and receiver from {0, 1, 2, 3, 4}:
sender ← RandomInt(0,4)
receiver ← RandomInt(0,4)
while receiver = sender do
receiver ← RandomInt(0,4)
Select a random amount between 1 and 150:
amount ← RandomInt(1, 150)
Create the transaction:
transaction ← {'sender': sender, 'receiver': receiver, 'amount' : amount}
Sign the transaction:
```

```
14: transaction.content ← String(transaction['sender']) + String(transaction['receiver']) +
String(transaction['amount'])
15: signature ← SHA256(transaction content)
16: transaction['signature'] ← signature
17: Add transaction to all nodes and increment epoch:
18: network.insert_element_all_nodes(transaction)
19: network.increment_epoch_all_nodes()
20: Simulate Byzantine fault in a random node:
21: network.corrupt_random_node(1)
22: Attempt to achieve consensus:
23: network.achieve_consensus()
24: for j ← 0 to 4 do
25: print SetChain of Node j : network.nodes[j].setchain.set, balance: network.nodes[j].balance
26: print "_____"
```

D. End Simulation

The end stage of the simulation loop being one of the major feature of the modeling and in making the decision as to whether to go for another cycle or not. Each loop can then represent a fixed amount of time, or transactions, such as a day of activity in the blockchain network. The decision criterion is then evaluated after each iteration; for modeling longer periods or particular situations, extended simulation is required, enabling the network to progress to more transactions, nodes and potential issues. If there is a pre-set number of iterations or transactions within the net to be met within the simulation then, the conclusion phase occurs, the network state is fixed, and data collected is made ready. ;In this regard, the "End Simulation" phase serves as a verification and a gatekeeping phase, which guarantees that the goals of the simulation are completed before proceeding with the evaluation.

E. Analysis

Upon concluding the simulation, the analysis phase ensues, playing a pivotal role in assessing the outcomes and understanding the implications of the simulation's results. This phase can be broadly categorized into two primary steps:

1) **Collect Metrics:** The aim of this stage is to gather all the critical metrics out of the simulation and record them in a suitable format. These metrics might include:
   - The aggregate level of transactions serviced during the course of the simulation.
   - Average transaction processing time, giving an indication of the efficiency of the network.
   - Average transaction fees that provide insights on the cost benefits of making transactions on this BC environment.
   - Profit or loss statistics for various nodes, which give a screen to the cost viability for those engaging in this organization
   - Any other relevant metric previously determined to be meaningful prior to running the simulation. These metrics not only measure what was going on in the simulation, but also serve as a starting point for more detailed experimental analysis.
2) **Analyze Results:** Armed with the accumulated metrics, the next step is to dissect, understand, and interpret them. The analysis could encompass:

- Evaluating the performance of the BC, ascertaining if it can handle real-world demands.
- Scrutinizing the security robustness of the network, especially in scenarios where adversarial behaviors were simulated.
- Gauging the economic dynamics, as if whether the rewards or fees incentivize honest participation and deter malicious activities.
- Drawing comparisons with benchmarks or other BC architectures, if applicable, to determine the relative strengths and weaknesses of the simulated setup.
- Identifying any unexpected behaviors or anomalies, which might hint at potential vulnerabilities or areas of improvement.

This deep dive into the results assists stakeholders in making informed decisions, whether that is adopting this particular BC setup, refining its parameters, or even reconsidering its viability based on the outcomes.

In essence, the analysis phase serves as the bridge between simulation and actionable insights, translating raw data into meaningful understanding that can guide future actions or decisions.

Technical Implementation of SetChain

The structure of epochs of the SetChain has optimized the ways of the transaction's operations and increases the system performance and capacity compared to the base Blockchain systems where all the transactions are linked to the blocks one by one. Unlike a sequential model, organically developed epochs create compound check points at predefined time horizons, reducing data duplication and time to retrieve the set. Operations occur over an epoch period where messages are collected, checked, and only those that are in the valid category are processed. The set of relevant blocks that includes only valid transactions is called a structured epoch; transactions with errors are detected throughout checks on balance, digital signatures, and consensus rules and stored in the block of intermediate results for further analysis. This classification mechanism enhances the utilization of C/R with discarding invalid transactions, cuts unnecessary network loads, increases scalability, storage, and general system implementation towards making SetChain more appropriate for the modern world blockchain networks.

4 Results

In our experiment, we examined the conduct of a decentralized network as far as the transactions and, specifically, the process of their validation is concerned. The network consists of nodes containing initial credits and has managed to incorporate solutions for Byzantine failures. Two scenarios were tested: one where Raw transaction validation and another in which data storage was done using pandas. The horizontal bars in Figure 4 represent the average number of transactions initiated by 20 nodes, ranging from about 440 to over 520. Evaluation resulted in finding quite high variation in number of transactions started at the nodes, implying that activity was not evenly distributed with some nodes participating in far more than 520 transactions having the maximum of 520 while few nodes exhibited low activity as low as nearly 450.

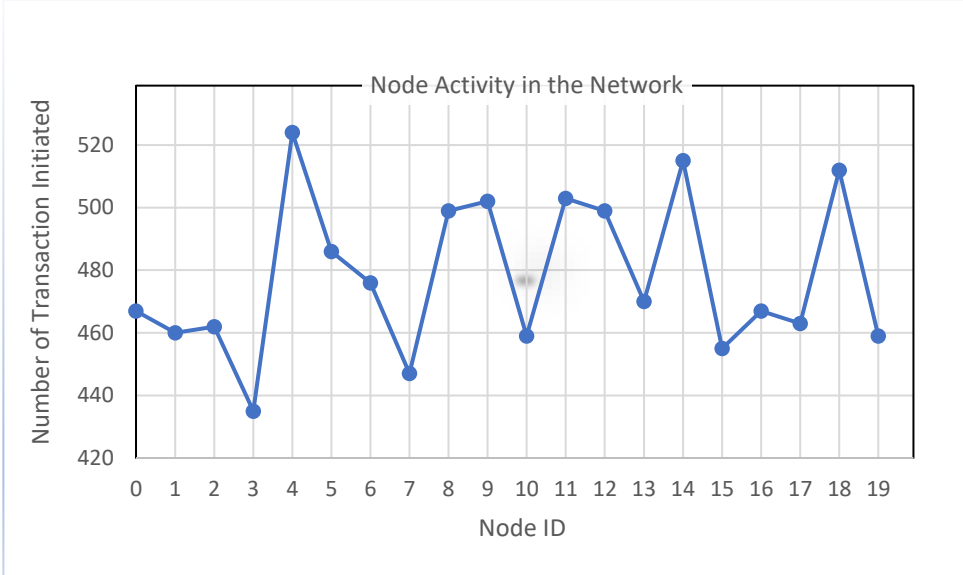


Figure 4: Node Activity in the Network

The peaks and troughs of the transaction rates graph indicate that some nodes start more transactions than others, whose amount may depend on the role assigned to the nodes in the network, their processing power, or even the network design in some cases prioritizes some node. The graph therefore represents a network with rich and varied activities across its nodes, suggesting unifying or distinctive degrees of freedom in the underlying graph structure or in its constituent nodes. A detailed analysis such as analyzing the temporal distribution of transactions and the network logs could provide the underlying mechanism of the network.

A. Transaction Validation

In our first scenario, we simulated 10,000 transactions across the network. Our results revealed that out of these, 4,934 transactions were considered valid while 66 transactions were deemed invalid. The invalid transactions mainly arose from nodes attempting to transfer amounts exceeding their balance. For instance, a transaction from node 0 to node 1 with an amount of 148 coins was invalid as node 0 only had a balance of 97 coins.

B. Data Storage

In the second scenario, our focus was on storing each transaction, whether valid or invalid, in a data frame using pandas as shown in algorithm 2.

Algorithm 2 Transaction Simulation and Analysis in a Network

```
valid_transactions ← 0
invalid_transactions ← 0
Initialize list to store transactions:
transactions ← list()
Initialize the network with 5 nodes and balance 50:
network ← Network(5, 50)
for i ← 1 to 1000 do
Select a random sender and receiver from {0, 1, 2, 3, 4}:
```

```
9: sender ← RandomInt(0,4)
10: receiver ← RandomInt(0,4)
11: while receiver = sender do
12: receiver ← RandomInt(0,4)
13: Select a random amount between 1 and 200:
14: amount ← RandomInt(1, 200)
15: Create the transaction:
16: transaction ← {'sender': sender, 'receiver': receiver, 'amount' : amount}
17: for node in network.nodes do
18: if transaction['sender'] != node.id and transaction['amount'] > node.balance
19: Print, "Transaction is invalid."
20: invalid_transactions ← invalid_transactions + 1
21: transaction['valid'] ← False else
22: node.insert_element(transaction)
23: valid_transactions ← valid_transactions + 1
24: transaction['valid'] ← True
25:
26: Add transaction to transactions list:
27: transactions.append(transaction)
28: network.increment_epoch_all_nodes()
29: Simulate Byzantine fault in random nodes:
30: network.corrupt_random_node(5)
31: Attempt to achieve consensus:
32: network.achieve_consensus()
33:
34: Convert list of transactions to a Data Frame:
35: df ← Data Frame(transactions)
```

This allowed for a more intricate analysis of each transaction. During the simulation, transactions were flagged as valid or invalid in real-time, and this information was appended to the dataframe. Our results here again reflected the challenges nodes faced in trying to execute transactions beyond their balance. For example, a transaction from node 0 to node 3 with an amount of 75 coins was marked invalid because node 0 only began with 50 coins.

C. Byzantine Faults

Incorporated in our simulation was the capability to introduce Byzantine faults. During each epoch, a random node was selected to behave maliciously. Our consensus mechanism, however, successfully identified and isolated these nodes, ensuring the integrity of our network.

D. Conclusion of Results

The simulation provided a clear view of how decentralized systems function, the importance of transaction validation, and the strength of consensus algorithms in maintaining system integrity despite adversarial conditions.

In a decentralized system, security is multifaceted. Our objective was not only to safeguard against external threats but also to ensure the integrity of transactions and data within the network. The following subsections detail the different layers and measures of security we integrated.

A. Cryptography and Transaction Signatures

Every transaction in our network was cryptographically signed (general methodology shown in figure 5) in by the sender's private key. This ensures two primary things:

- Authenticity: Verifying that the sender genuinely initiated the transaction.
- Non-repudiation: Ensuring that once the transaction has been made, the sender cannot deny having made it.

Nodes in the network used public keys to verify the signature of each transaction, ensuring its legitimacy.

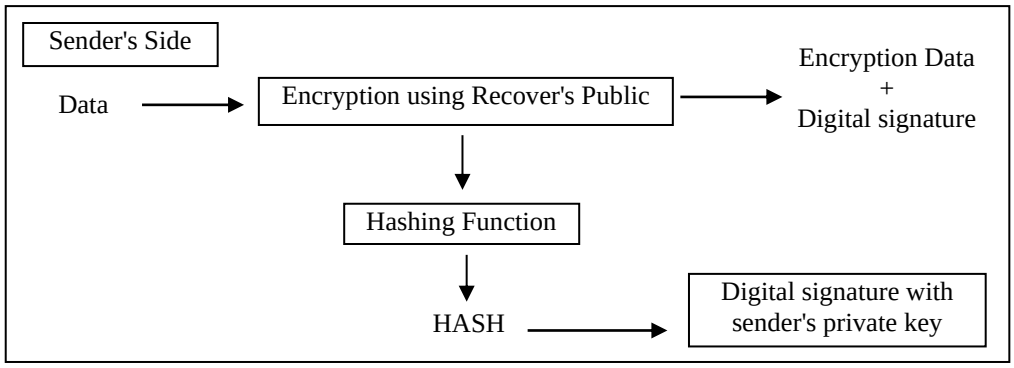


Figure 5: Signature General Methodology (Sasi et al., 2023)

B. Consensus Mechanisms

The decentralized network employed a Proof of Work (PoW) consensus mechanism as illustrate in figure 6. This requires nodes to solve a cryptographic puzzle, which acts as a deterrent for malicious actors. This system not only validates and approves legitimate transactions but also makes any adversarial attempt to alter transaction records computationally intensive and hence, unfeasible.

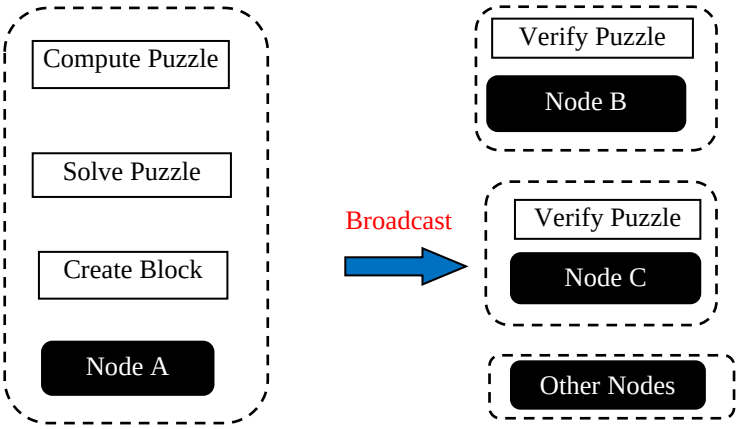


Figure 6: General Methodology of Consensus Mechanism of PoW (Chinnasamy et al., 2021)

C. Byzantine Fault Tolerance

To address the challenge of Byzantine faults, where nodes might behave maliciously or transmit incorrect information, our network was equipped with Byzantine fault tolerance algorithms. This ensured that even if a certain percentage of nodes acted maliciously, the integrity and functionality of

the system were not compromised. Malicious nodes were identified and isolated from the network, thus preserving trustworthiness.

D. Secure Data Storage

By incorporating data storage using pandas, every transaction's details, whether valid or invalid, were securely stored. Periodic hashing and backup mechanisms ensured that the transaction data remained consistent and unchanged. In addition, through encryption techniques, the stored data was safeguarded from unauthorized access.

E. Conclusion on Security

Ensuring security in a decentralized network is an ongoing challenge. However, through a combination of cryptographic techniques, robust consensus mechanisms, and advanced monitoring, our network

Comparative Analysis with Other Blockchain Solutions

In the table 3 below, it is demonstrated that Ethereum, Hyperledger Fabric, Optimistic and ZK-Rollups are comparatively more decentralized, scalable and secure than the aforementioned blockchains, albeit at the cost of low throughput, high transaction fees and data synchronization issues. SetChain presents a new architecture of distributed ledgers that improves scalability, fault tolerance and data organization based on the notions of epochs and transaction type, eliminating duplicates and minimizing computational overhead. Nonetheless, it can make systems integration with old-fashioned software more challenging and storing of information for high traffic networks may need more memory than before. The employment of various approaches to consensus, as seen in BFT and PoW, complicates the system but might have more enhanced results when more developments are made.

Table 3: Comparative Analysis of SetChain with Existing Blockchain Solutions

Metric	Ethereum	Hyperledger Fabric	Layer 2 Solutions	SetChain
Scalability	Low (20-30 TPS)	Moderate (1,000-10,000 TPS)	High (up to 2,000 TPS, off-chain)	High (structured epochs enable efficient scalability)
Fault Tolerance	High (PoW and PoS mechanisms)	Moderate (permissioned network)	Moderate (dependent on main chain)	High (Byzantine Fault Tolerance and flexible consensus mechanisms)
Consensus Efficiency	Energy-intensive (PoW)	Efficient but centralized (PBFT)	High efficiency (off-chain)	Efficient and flexible (customizable consensus mechanisms)
Transaction Throughput	Low (limited by PoW/block size)	High (optimized for enterprise)	High (aggregation improves throughput)	High (optimized through structured epochs)
Data Storage Optimization	Linear and redundant storage	Improved but centralized	Moderate (partial off-chain storage)	Optimized (structured epochs reduce redundancy)
Decentralization	Fully decentralized	Partially decentralized	Partially decentralized	Fully decentralized
Latency	High (block time delays)	Low	Low (off-chain operations)	Low (efficient transaction validation and categorization)
Energy Consumption	High due to PoW	Low	Low	Moderate (customizable consensus reduces overhead)
Complexity	High (smart contracts, PoW)	Moderate (permissioned setup)	High (off-chain validation required)	Moderate (simplified through epochs and categorization)

5 Discussion

The findings demonstrate how SetChain improves main blockchain frameworks specifically in terms of scalability, database management, and transactions. The list of advantages over traditional blockchains such as Ethereum is explained by the fact that SetChain combines transactions into definite chronological intervals that reduces the number of repeated data inquiries and eliminates the problem of network overload and great time delay. Transaction categorization mechanism also contributes to performance enhancement because valid transaction is separated from the invalid of transaction to minimize computational time and reduce potential delay of system. The simulations illustrated SetChain's high throughputs in the validation of the high numbers of transactions, where out of the 10,000 tested transactions, 4934 were valid and passed while the Byzantine failure tolerance was evidenced by the ability of isolating the malicious nodes in maintaining the networks integrity. While Layer 2 solutions require off-chain computations, SetChain brings on-chain scalability, which prevents tradoffs and presents the framework as a suitable for building high-performance and reliable decentralized applications.

6 Conclusion

The SetChain provides a possible solution to the key problem of the BC technology, while paying more attention to the problems of data storage and system scalability. The use of the structured epoch in creating indexes for the transactions make it foul proof, efficient and scalable on data storage. Transaction signatures again are additionally incorporated into the integrated system as the definitive means of maintaining the identity and confidentiality of the transaction. Moreover, the application of consensus mechanisms amplifies the reliability and solidity of the system making set chain ideal for real use.

The simulations described in this work were performed on a decentralized network of 20 nodes; such a network architecture was due to the current scant computational resources at our disposal. As in any implementation of a blockchain-based system, it is worth mentioning that our setting shows the concept and possibility of SetChain at its best; however, scaling it up needs to be investigated further. Therefore, more research and development of networks with more nodes are needed so that we can further determine how SetChain works in more practical contexts of real-world large-node decentralized systems. It seems that with SetChain's approach the tradeoff between storing data and handling an increasing number of transactions is quite fair and therefore is well suitable for BC networks that are to extend the number of transactions in future. Thus, intended for enhancement of the identified directions of BC application, with resulting benefits and innovative features, SetChain becomes an attractive solution for increasing the effectiveness and security of BC networks for the creation and development of DEPP and other applications.

References

[1] Abdullah, M. (2023). Effect of After-Sale Services on Customer Satisfaction and Loyalty in Automation Company Case Cimcorp.

[2] Al Mamun, A., Faruk Jahangir, M. U., Azam, S., Kaiser, M. S., & Karim, A. (2021). A combined framework of interplanetary file system and blockchain to securely manage electronic medical records. In *Proceedings of International Conference on Trends in Computational and Cognitive Engineering: Proceedings of TCCE 2020* (pp. 501-511). Springer Singapore. https://doi.org/10.1007/978-981-33-4673-4_40

[3] Al_Barazanchi, I., Murthy, A., Al Rababah, A. A., Khader, G., Abdulshaheed, H. R., Rauf, H. T., ... & Niu, Y. (2022). Blockchain technology-based solutions for IOT security. *Iraqi Journal for Computer Science and Mathematics*, *3*(1), 53-63. https://doi.org/10.52866/ijcsm.2022.01.01.006

[4] Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University-Computer and Information Sciences*, *34*(10), 8176-8206. https://doi.org/10.1016/j.jksuci.2022.08.003

[5] Bandari, V. (2023). Enterprise data security measures: a comparative review of effectiveness and risks across different industries and organization types. *International Journal of Business Intelligence and Big Data Analytics*, *6*(1), 1-11.

[6] Campos, E. M., Saura, P. F., González-Vidal, A., Hernández-Ramos, J. L., Bernabe, J. B., Baldini, G., & Skarmeta, A. (2022). Evaluating Federated Learning for intrusion detection in Internet of Things: Review and challenges. *Computer Networks*, *203*, 108661. https://doi.org/10.1016/j.comnet.2021.108661

[7] Cheng, L. W., & Wei, B. L. (2024). Transforming smart devices and networks using blockchain for IoT. *Progress in Electronics and Communication Engineering, 2*(1), 60–67. https://doi.org/10.31838/PECE/02.01.06

[8] Chinnasamy, P., Vinothini, C., Arun Kumar, S., Allwyn Sundarraj, A., Annlin Jeba, S. V., & Praveena, V. (2021). Blockchain technology in smart-cities. In *Blockchain technology: Applications and challenges* (pp. 179-200). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-69395-4_11

[9] Clementine, G., Willy, S., Thomas, P., Kaitai, L., & Duncan, S.W. (2014). Empowering Personal Health Records with Cloud Computing. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 5*(4), 3-28.

[10] Dedeoglu, V., Dorri, A., Jurdak, R., Michelin, R. A., Lunardi, R. C., Kanhere, S. S., & Zorzo, A. F. (2020, January). A journey in applying blockchain for cyberphysical systems. In *2020 International Conference on COMmunication Systems & NETworkS (COMSNETS)* (pp. 383-390). IEEE. https://doi.org/10.1109/COMSNETS48256.2020.9027487

[11] Devaraj, A. F. S., Elhoseny, M., Dhanasekaran, S., Lydia, E. L., & Shankar, K. (2020). Hybridization of firefly and improved multi-objective particle swarm optimization algorithm for energy efficient load balancing in cloud computing environments. *Journal of Parallel and Distributed Computing*, *142*, 36-45. https://doi.org/10.1016/j.jpdc.2020.03.022

[12] Faruk, M. J. H., Shahriar, H., Valero, M., Sneha, S., Ahamed, S. I., & Rahman, M. (2021, September). Towards blockchain-based secure data management for remote patient monitoring. In *2021 IEEE international conference on digital health (ICDH)* (pp. 299-308). IEEE. https://doi.org/10.1109/ICDH52753.2021.00054

[13] Goyat, R., Kumar, G., Alazab, M., Conti, M., Rai, M. K., Thomas, R., ... & Kim, T. H. (2020). Blockchain-based data storage with privacy and authentication in internet of things. *IEEE Internet of Things Journal*, *9*(16), 14203-14215. https://doi.org/10.1109/JIOT.2020.3019074

[14] Haber, E., & Reichman, A. (2020). The User, the Superuser, and the Regulator: Functional Separation of Powers and the Plurality of the State in Cyber. *Berkeley Tech. LJ*, *35*, 431. https://doi.org/10.15779/Z38V40K05C

[15] Hafid, A., Hafid, A. S., & Samih, M. (2020). Scaling blockchains: A comprehensive survey. *IEEE access*, *8*, 125244-125262. https://doi.org/10.1109/ACCESS.2020.3007251

[16] Haque, E. U., Shah, A., Iqbal, J., Ullah, S. S., Alroobaea, R., & Hussain, S. (2024). A scalable blockchain based framework for efficient IoT data management using lightweight consensus. *Scientific Reports*, *14*(1), 7841. https://doi.org/10.1038/s41598-024-58578-7

[17] He, Q., & He, H. (2020). A novel method to enhance sustainable systems security in cloud computing based on the combination of encryption and data mining. *Sustainability, 13*(1), 101. https://doi.org/10.3390/su13010101

[18] Idowu, A. O., & Eiriemiokhale (CLN), K. A. (2020). Availability and Awareness of Electronic Databases for Teaching and Research by Lecturers in Public Universities in South-West, Nigeria. *Indian Journal of Information Sources and Services*, *10*(1), 27–35. https://doi.org/10.51983/ijiss.2020.10.1.481

[19] Krishnaraj, N., Elhoseny, M., Lydia, E. L., Shankar, K., & ALDabbas, O. (2021). An efficient radix trie-based semantic visual indexing model for large-scale image retrieval in cloud environment. *Software: Practice and Experience*, *51*(3), 489-502. https://doi.org/10.1002/spe.2834

[20] Lakshmi, V. S., Deepthi, S., & Deepthi, P. P. (2021). Collusion resistant secret sharing scheme for secure data storage and processing over cloud. *Journal of Information Security and Applications*, *60*, 102869. https://doi.org/10.1016/j.jisa.2021.102869

[21] Mızrak, F. (2023). Use of big data in strategic management as a new perspective. In *New Perspectives and Possibilities in Strategic Management in the 21st Century: Between Tradition and Modernity* (pp. 409-425). IGI Global. https://doi.org/10.4018/978-1-6684-9261-1.ch020

[22] Nihlani, A., & Chhabda, P. K. (2024). The Impact of Digital Transformation on Supply Chain Management: A Study of How Firms Adapt. *Indian Journal of Information Sources and Services*, *14*(4), 1–6. https://doi.org/10.51983/ijiss-2024.14.4.01

[23] Oliva, G. A., Hassan, A. E., & Jiang, Z. M. (2020). An exploratory study of smart contracts in the Ethereum blockchain platform. *Empirical Software Engineering*, *25*, 1864-1904. https://doi.org/10.1007/s10664-019-09796-5

[24] Oyinloye, D. P., Teh, J. S., Jamil, N., & Alawida, M. (2021). Blockchain consensus: An overview of alternative protocols. *Symmetry*, *13*(8), 1363. https://doi.org/10.3390/sym13081363

[25] Pozi, M. S. M., & Omar, M. H. (2020). A Kernel Density Estimation Method to Generate Synthetic Shifted Datasets in Privacy-Preserving Task. *Journal of Internet Services and Information Security*, *10*(4), 70-89. https://doi.org/10.22667/JISIS.2020.11.30.070

[26] Premkamal, P. K., Pasupuleti, S. K., Singh, A. K., & Alphonse, P. J. A. (2021). Enhanced attribute based access control with secure deduplication for big data storage in cloud. *Peer-to-Peer Networking and Applications*, *14*, 102-120. https://doi.org/10.1007/s12083-020-00940-3

[27] Prusty, N. (2017). Building Blockchain Projects. *Packt Publishing*.

[28] Qalati, S. A., Ostic, D., Sulaiman, M. A. B. A., Gopang, A. A., & Khan, A. (2022). Social media and SMEs' performance in developing countries: Effects of technological-organizational-environmental factors on the adoption of social media. *Sage Open*, *12*(2), 21582440221094594. https://doi.org/10.1177/21582440221094594

[29] Reimer, L. C., Sardà Carbasse, J., Koblitz, J., Ebeling, C., Podstawka, A., & Overmann, J. (2022). Bac Dive in 2022: the knowledge base for standardized bacterial and archaeal data. *Nucleic Acids Research*, *50*(D1), D741-D746. https://doi.org/10.1093/nar/gkab961

[30] Rejeb, A., Suhaiza, Z., Rejeb, K., Seuring, S., & Treiblmaier, H. (2022). The Internet of Things and the circular economy: A systematic literature review and research agenda. *Journal of Cleaner Production*, *350*, 131439. https://doi.org/10.1016/j.jclepro.2022.131439

[31] Safkhani, M., Camara, C., Peris-Lopez, P., & Bagheri, N. (2021). RSEAP2: An enhanced version of RSEAP, an RFID based authentication protocol for vehicular cloud computing. *Vehicular Communications*, *28*, 100311. https://doi.org/10.1016/j.vehcom.2020.100311

[32] Sagheer, A., & Dawood, O. (2021). Survey:(Blockchain-Based Solution for COVID-19 and Smart Contract Healthcare Certification). *Iraqi Journal for Computer Science and Mathematics*, *2*(1), 1-8.

[33] Said, N. M. M., Ali, S. M., Shaik, N., Begum, K. M. J., Shaban, A. A. A. E., & Samuel, B. E. (2024). Analysis of Internet of Things to Enhance Security Using Artificial Intelligence based Algorithm. *Journal of Internet Services and Information Security*, *14*(4), 590-604. https://doi.org/10.58346/JISIS.2024.I4.037

[34] Salman, S. A., Janabi, S. A., & Sagheer, A. M. (2023). Security attacks on e-voting system using blockchain. *Iraqi Journal for Computer Science and Mathematics*, *4*(2), 16. https://doi.org/10.52866/ijcsm.2023.02.02.016

[35] Sasi, S., Subbu, S. B. V., Manoharan, P., & Abualigah, L. (2023). Design and implementation of secured file delivery protocol using enhanced elliptic curve cryptography for class I and class II transactions. *Journal of Autonomous Intelligence*, *6*(3).

[36] Sund, T., Lööf, C., Nadjm-Tehrani, S., & Asplund, M. (2020). Blockchain-based event processing in supply chains—A case study at IKEA. *Robotics and Computer-Integrated Manufacturing*, *65*, 101971. https://doi.org/10.1016/j.rcim.2020.101971

[37] Sunyaev, A., & Sunyaev, A. (2020). Cloud computing. *Internet computing: Principles of distributed systems and emerging internet-based technologies*, 195-236.

[38] Uvarajan, K. P. (2024). Integration of blockchain technology with wireless sensor networks for enhanced IoT security. *Journal of Wireless Sensor Networks and IoT*, *1*(1), 23-30. https://doi.org/10.31838/WSNIOT/01.01.04

[39] Velliangiri, A. (2024). Security challenges and solutions in IoT-based wireless sensor networks. *Journal of Wireless Sensor Networks and IoT*, *1*(1), 8-14. https://doi.org/10.31838/WSNIOT/01.01.02

[40] Velmurugan Vaithiyanathan, Venkatesan Mani, **Suresh Govindasamy** & Jaisiva Selvaraj (2024) "A Multi-Objective Time – Series Optimization for Optimum Planning Design of Integrative Power System with the Effects of Multi-Dimensional Sources of Uncertainty", Electric Power Components and Systems, 52:6, 891-904, 2023, DOI: 10.1080/15325008.2023.2237017.

[41] Wang, J., Chen, J., Xiong, N., Alfarraj, O., Tolba, A., & Ren, Y. (2023). S-BDS: An effective blockchain-based data storage scheme in zero-trust IoT. *ACM Transactions on Internet Technology*, *23*(3), 1-23. https://doi.org/10.1145/3511902

[42] Wang, Y., Liu, H., Wang, J., & Wang, S. (2020, December). Efficient data interaction of blockchain smart contract with oracle mechanism. In *2020 IEEE 9th Joint International Information Technology and Artificial Intelligence Conference (ITAIC)* (Vol. 9, pp. 1000-1003). IEEE. https://doi.org/10.1109/ITAIC49862.2020.9338784

[43] Wei, P., Wang, D., Zhao, Y., Tyagi, S. K. S., & Kumar, N. (2020). Blockchain data-based cloud data integrity protection mechanism. *Future Generation Computer Systems*, *102*, 902-911. https://doi.org/10.1016/j.future.2019.09.028

[44] Wu, C., Xiong, J., Xiong, H., Zhao, Y., & Yi, W. (2022). A review on recent progress of smart contract in blockchain. *IEEE Access*, *10*, 50839-50863. https://doi.org/10.1109/ACCESS.2022.3174052

[45] Xu, X., Chen, Y., Yuan, Y., Huang, T., Zhang, X., & Qi, L. (2020). Blockchain-based cloudlet management for multimedia workflow in mobile cloud computing. *Multimedia Tools and Applications*, *79*, 9819-9844. https://doi.org/10.1007/s11042-019-07900-x

[46] Yalcinkaya, E., Maffei, A., & Onori, M. (2020). Blockchain reference system architecture description for the ISA95 compliant traditional and smart manufacturing systems. *Sensors*, *20*(22), 6456. https://doi.org/10.3390/s20226456

[47] Yu, K., Tan, L., Aloqaily, M., Yang, H., & Jararweh, Y. (2021). Blockchain-enhanced data sharing with traceable and direct revocation in IIoT. *IEEE transactions on industrial informatics*, *17*(11), 7669-7678. https://doi.org/10.1109/TII.2021.3049141

[48] Yusoff, M. N. B., & Abd Ali, S. M. (2024). Bitcoin Layer Two Scaling Solutions: Lightening Payment Channels Network Comprehensive Review, Mechanisms, Challenges, Open Issues and Future Research Directions. *Iraqi Journal for Computer Science and Mathematics*, *5*(1), 25-59. https://doi.org/10.52866/ijcsm.2024.05.01.003

[49] Zhou, Q., Huang, H., Zheng, Z., & Bian, J. (2020). Solutions to scalability of blockchain: A survey. *IEEE Access*, *8*, 16440-16455. https://doi.org/10.1109/ACCESS.2020.2967218

Authors Biography

Firas Abdulrahman Yousif is an Assist Lecturer at the Department of Computer Science in the Faculty of Education of University of Al-Hamdaniya, Iraq. He holds his B.Sc. and M.Sc. in computer technical engineering from Northern Technical University, Mosul, Iraq in 2005 and 2009, respectively. His main research areas of interest include IOT, Artificial Intelligence, and network.

Mariam Raheem Mirza is an Assist Lecturer at the Department of Computer Science in the Faculty of Education of University of Al-Hamdaniya, Iraq. She received a Bachelor of Electrical Engineering in 2008 from University of Anbar, Iraq, followed by an M.Sc. in Digital Communications Networks Engineering in 2016 from the University of Leeds, UK. Her main research includes image processing, computer vision and pattern recognition.