Gracy, M, Balasundaram, Rebecca and Raj, S. Albert Antony (2023) Enhancing Data Integrity in Blockchain through Fuzzy Augmented Lagrangian Optimization and Compact Blocks to Minimize Redundancy. International Journal of Intelligent Systems and Applications in Engineering (IJISAE), 11 (4).

International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Enhancing Data Integrity in Blockchain through Fuzzy Augmented Lagrangian Optimization and Compact Blocks to Minimize Redundancy

M. Gracy[1*], Rebecca Jeyavadhanam Balasundaram[2], S. Albert Antony Raj[3]

Submitted: 08/05/2023 **Revised**: 17/07/2023 **Accepted**: 06/08/2023

Abstract*:* Blockchain is a method of storing data that makes it difficult or impossible to modify, steal, or swindle the system. Every block in a blockchain has its header with the unique nonce, timestamp, hash, the previous hash, transaction data, and the Merkle root. The Merkle tree is crucial in a block for consolidating data into a single hash, but it can suffer from data redundancy concerns during its structure formation. The central focus of the paper revolves around data redundancy and presents a novel approach for ensuring data integrity in blockchain with a compactness technique. Compactness is accomplished using Fuzzy Augmented Lagrangian Optimization to reduce data redundancy (FALORR). We integrate compact blocks into regular blockchain setup, bringing out a faster and more efficient way to reduce memory requirements. This effectual transaction verification structure improves the overall security and efficiency of the blockchain network by detecting and preventing malicious activities. To evaluate the effectiveness of the proposed system, we employed Hyperledger Caliper, a specialized benchmarking tool tailored for gauging the performance of blockchain solutions. The results of our implementation and evaluation demonstrate the effectiveness of the proposed structure in minimizing data redundancy and maintaining the data integrity of transactions in the blockchain system.

Keywords: *Blockchain, Compact blocks, Merkle Tree, Augmented Lagrangian Optimization, Data Redundancy.*

1. Introduction

Blockchain is a technology that is rapidly gaining prominence and promise. [1] [2] [3] Supporters of blockchain technology propose that it has a vast range of potential applications across diverse industries, including but not limited to banking, supply-chain management, energy, Internet of Things (IoT), healthcare, media, government, and various others [4] [5][6] [7] [8] [9]. Blockchain is a decentralized and distributed digital ledger technology that enables secure and transparent record-keeping of transactions across a network of computers. Each transaction is cryptographically linked to the previous one, forming a chain of blocks. The first block in the decentralized blockchain is called the genesis block, and it was intellectualized by a person (or set of people) known as Satoshi Nakamoto in 2008[10]. The typical blockchain structure is shown in Fig 1.

Block Header: The metadata of a blockchain block containing necessary information like the timestamp, the previous block's hash, and a nonce used in mining.

Nonce: A random value used in mining to adjust the block's hash and meet the network's difficulty benchmarks, ensuring consensus while adding a new block.

Timestamp: The recorded time when a block is created, aiding in maintaining sequential order and avoiding manipulation.

Hash: A fixed-length alphanumeric string representing the unique digital fingerprint of a block's data, ensuring integrity and security.

Previous Hash: The hash of the prior block in the chain, linking blocks together and forming a sequential structure.

Transaction Data: Records of cryptocurrency transactions or other relevant data stored within a block, forming the core purpose of the blockchain.

Merkle Root: A cryptographic hash of all transaction data in a block, facilitating efficient verification of contained transactions and preserving the block's integrity.

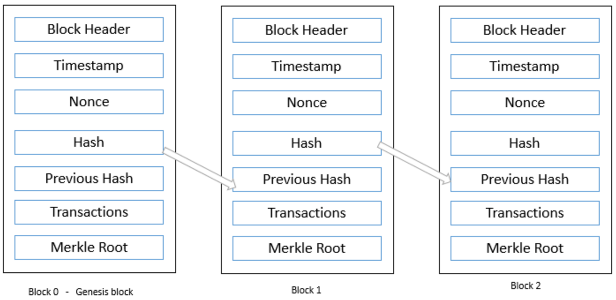


Fig 1. A Typical Blockchain structure

Merkle trees [11] [12] [13] ensure data integrity and efficient verification within this structure. Merkle trees use

[1]*Dept of Comp Appln, CSH, SRMIST, Kattankulathur – 603403, INDIA*
ORCID ID: 0000-0002-2933-4210
[2]*Dept of Comp Science, York St John University London, UK*
ORCID ID: 0000-0001-6618-2642
[3]*Dept of Comp Appln, CSH, SRMIST, Kattankulathur – 603403, INDIA*
ORCID ID: 0000-0003-0363-4247
** Corresponding Author Email: gm3064@srmist.edu.in*

cryptographic hashing to represent large amounts of data by aggregating it into a single hash value, reducing storage and enhancing security. [14] The Merkle tree structure is shown in Fig 2. For individuals, the act of storing data within a blockchain environment offers a host of advantages. These include alleviating the burden on local storage resources, minimizing the risk of third-party interference, and facilitating remote accessibility. However, adopting Merkle tree storage while providing convenience also introduces a set of corresponding challenges, notably including highly sensitive data results in increased energy consumption, the potential for selfish mining-induced forks, and exposure to multiple threats within intricate computational landscapes. While the conventional Merkle tree mechanism serves its intended purpose, it has its drawbacks, primarily revolving around the issue of data redundancy. Each transaction necessitates a corresponding hash value, and a typical block can accommodate approximately 4000 transactions. These transactions are paired sequentially through each level until they culminate at the root. In cases where unpaired nodes remain, duplication is imperative to establish proper pairing, a process that persists until a solitary node reaches the root. A typical blockchain consists of several components like block header, nonce, timestamp, hash, previous hash, transaction data, and Merkle root. The traditional Merkle tree set up in the blockchain network is shown in Fig 3.

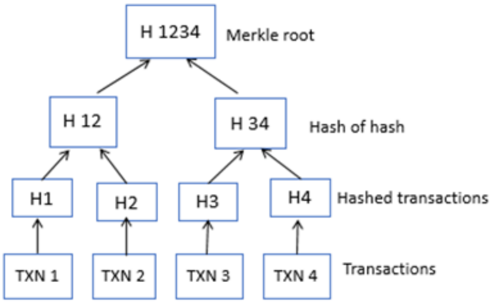


Fig 2. Merkle Tree Structure

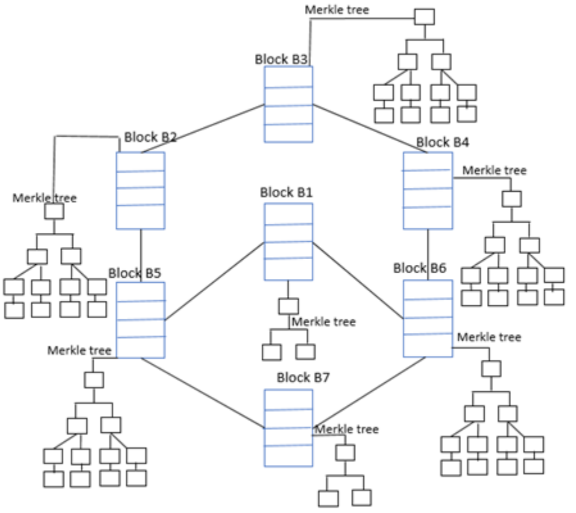


Fig 3. Merkle tree in the blockchain network

The focal point of the proposed research is thoughtfully centered on addressing this duplication predicament. The outcome is a robust solution presented as a data integrity framework. Building upon our prior work involving pruned Merkle trees, effectively eliminating duplicated nodes, this endeavor strives to elevate data integrity. The primary objective is to eradicate data redundancy with a high degree of efficiency decisively. This work underscores the significance of optimizing data storage through blockchain while navigating the intricacies of Merkle tree structures. It offers a pioneering approach to resolving duplication, further enhancing data integrity within the blockchain context.

The fundamental aspect of maintaining data integrity hinges on the trust established between the user and the transaction ledger. Our suggested method of node pairing aims to decrease data redundancy. We showcased the assurance of data integrity by incorporating 'compact blocks' [15] within the blockchain. Incorporating compact blocks into the blockchain system offers significant benefits in our pursuit of minimizing data redundancy. In the upcoming sections, we will delve deeper into the concept of 'compact blocks' for a more comprehensive understanding.

The highpoints of our contributions in this paper can be concisely summarized as follows:

1. This paper introduces a novel protocol to verify data integrity, utilizing a Fuzzy Augmented Lagrangian Optimization approach. The algorithm can effectively counteract data redundancy in the context of redundancy labels (RL) tagging. This is achieved by pairing hash nodes within the generation of the Merkle tree within a given block. The proposed protocol enhances the overall integrity of the data by minimizing redundancy, which in turn contributes to a more efficient and secure blockchain system.
2. This paper presents the introduction of a Compact Block Relay protocol, which involves the integration of compact blocks into a ledger. This strategic inclusion of compact blocks yields a notable reduction in memory requirements compared to the standard blocks. This innovative concept facilitates a swifter and more efficient data communication mode within the network while concurrently decreasing the demand for memory resources. As a result, adopting this protocol can significantly enhance the network's overall performance and resource utilization, contributing to a more streamlined and optimized blockchain ecosystem.
3. This paper assesses the performance of the suggested approach across various metrics, including throughput, security, memory utilization, authentication time, energy consumption, and processing time. The conducted experiments aim to compare the proposed

FALORR method with established techniques. The empirical findings consistently indicate the efficacy of the FALORR method across all evaluated parameters, underscoring its effectiveness in enhancing performance and addressing key aspects of concern.

The rest of the paper is structured as follows. Section 2 provides an overview of the related work. Section 3 introduces the preliminaries. Section 4 describes the proposed system in detail. Section 5 has experimental results and analysis of the proposed scheme. Section 6 presents the performance analysis of the scheme. Section 7 concludes the paper with future directions.

2. Overview of the Related work

This section discusses research studies that ensure data integrity through various approaches and principles.

2.1. Data integrity verification

Data integrity verification is a crucial aspect of blockchain technology. Ensuring data integrity within a blockchain system is fundamental to maintaining trust, security, and the reliability of the information stored on the chain. In their methodology, Rosco et al. [16] operate under the assumption that the raw data is stored in a distinct location from the blockchain system. They enable the submission of a data identifier and its corresponding hash onto the blockchain. This hash serves as a means to verify the integrity of the original data, a process that can be executed whenever needed. The study outlines a range of applications where blockchain-based hash validation proves beneficial. To empirically validate their approach, the researchers integrate it into an application's audit trail, demonstrating its efficacy in validating the data contained within the audit trail. To tackle the issue of deliberate data tampering, Choi et al. [17] introduce an innovative framework for overseeing the data integrity of Logic Controllers through the application of blockchain technology. With a focus on the context of a nuclear power plant setting, the researchers devised a closed-off blockchain system tailored to supervise the data integrity of these logic controllers. A fresh approach to monitoring the data integrity was conceptualized. In their paper [18] the authors present an innovative system of interconnected blockchain organized in a decentralized hierarchy. This system is designed to guarantee data integrity and facilitate seamless blockchain interoperability effectively. The primary objective is to solve the hurdles diverse smart city entities and organizations encounter. The paper proposed by Lei et al. [19] suggests an amalgamated Internet of Things (IoT) platform employing blockchain technology to ensure the integrity of sensing data. The primary objective of this platform is to furnish device owners with a user-friendly application that offers an all-encompassing and unchangeable record, facilitating convenient access to their devices utilized across diverse domains. In his paper, Tanvir [20] presents a conceptual framework for a blockchain-based data integrity service using Big Data techniques to manage IoT device data within smart cities. The author sourced essential information from multiple references and employed three distinct assessments to gauge important performance metrics. Data segregation was achieved by utilizing the K-means algorithm while establishing secure communication among IoT devices was achieved by implementing a blockchain approach.

2.2. Merkle tree

As the adoption of blockchain technology continues to surge, Merkle trees, also known as hash trees, are assuming pivotal roles in the verification and retrieval of data. They are integral to implementing blockchain systems, enabling streamlined and secure verification of extensive data structure contents. Hariharasitaraman et al. [21] introduce an innovative technique that is publicly verifiable and ensures the integrity of medical records stored in the cloud while enhancing data security. This method relies on a position-aware Merkle tree framework with a 3-tuple scheme. This scheme's effectiveness in delivering authentication and data integrity services has been validated, highlighting its resilience. Mohan et al. [22] introduced a novel system for auditing cloud data, which combines Merkle Tree-based cloud auditing with a blockchain-based audit recording mechanism. The fundamental concept revolves around capturing each verification outcome as a transaction within the blockchain. Leveraging the inherent time-sensitive properties of blockchain, verifications are timestamped once their corresponding transactions are included in the blockchain. This design empowers users to validate whether auditors conducted verifications at the designated times. Mizrahi et al. [23] leverage the inherent traits of transactions to enhance the arrangement of Merkle trees, thus enhancing the efficiency of blockchain networks. The primary emphasis is optimizing the handling of routine transaction processes, where Merkle proofs are concurrently furnished for many accounts. The paper establishes a baseline for the minimum communication expenses and introduces algorithms that capitalize on traffic patterns to substantially curtail these costs. In their paper, Liu et al. [11] comprehensively explores Merkle trees, delving into their fundamental principles, inherent properties, notable benefits, and diverse applications.

2.3. Fuzzy Augmented Lagrangian Optimization

The Fuzzy Augmented Lagrangian Optimization approach solves optimization problems with equality and inequality constraints. It combines the concepts of Augmented Lagrangian Optimization and fuzzy logic to handle problems where the constraints might not be satisfied exactly but within a certain tolerance level. This approach is particularly useful when traditional optimization methods struggle to find feasible solutions due to constraints that are difficult to satisfy precisely. Zhang et al. [24] proposed the Augmented Lagrangian coordination optimization method to solve the energy-optimal SMS allocation problem. The energy-optimal SMS allocation model is constructed and decomposed into several loose-coupled and distributed elements. Two variants of the Augmented Lagrangian coordination method are implemented to formulate the proposed problem and obtain final SMS allocation results. The research conducted by Geng Zhang et al. [25] studies a Manufacturing Service Configuration problem considering the decision autonomy and limited production capacities of cloud service providers. Augmented Lagrangian coordination optimization method can support open-structure collaboration and allow participants to maintain decision autonomy and in their paper, it is extended to solve the proposed configuration problem by the introduction of a coordination element. Dhavamani et al. [26] introduced the concept of utilizing the augmented Lagrangian function to enhance the longevity of IoT networks. This involves diminishing the energy demands of extensive IoT nodes and achieving equilibrium in the distribution of traffic loads.

2.4. Blockchain Application

Blockchain is a distributed and decentralized digital ledger that records transactions or data securely and tamper-evidently. Great achievements have been made in exploring the application of blockchain in crypto transactions. In their paper, Habib et al. [27] extensively examine the evolution of blockchain technology, meticulously exploring its various applications and advantages. Special focus is placed on dissecting the intricacies of public key cryptography within the blockchain, delving into the realm of distributed transaction ledgers, and addressing the hurdles encountered in this domain. An exhaustive compilation of Blockchain’s diverse applications within the financial transaction system is also presented. Joo et al. [28] demonstrated the significant contributions of blockchain technology to the realm of finance as a whole. They explored various domains within finance to uncover opportunities where this technology could exert a more substantial influence, particularly in the area of payment systems. Bao et al. [29] conducted a comprehensive examination of the potential applications of blockchain technology within the energy sector. This encompassed a broad spectrum of functions including energy management, peer-to-peer trading, electric vehicle integration, and addressing carbon emissions. The authors also highlighted the security and privacy hurdles this technology encounters. Sunny et al. [30] comprehensively explores the attributes, operational methods, and uses of blockchain across diverse sectors including transportation, commerce, industry, privacy and security, finance, government, education, healthcare, and the Internet of Things (IoT). They outlined the primary focal points of research covered in the existing literature within each application domain and showed prospective avenues for future research in these domains. Ozdemir et al. [31] have introduced an all-encompassing criteria framework designed to evaluate the fundamental components of blockchain technology. They have conducted an exploratory study within the realm of travel and tourism, harnessing cutting-edge instruments such as smart contracts, decentralized applications, and cryptocurrencies. This systematic approach empowers decision-makers with the capacity to proficiently assess a wide array of Distributed Applications (DAPPs).

The inherent qualities of sincerity, transparency, and data traceability embedded in blockchain technology have established its pivotal significance across domains such as finance, government, healthcare, and the Internet of Things (IoT). Within this landscape, the Merkle tree structure assumes a crucial role in ensuring data integrity verification, where it amalgamates data security and data redundancy. This facet remains an area of active investigation. Consequently, this research introduces an approach to validate data integrity within the context of Merkle tree construction in blockchain environments. The method leverages fuzzy augmented Lagrangian optimization to address the challenge of data redundancy while fostering data security.

3. Preliminaries

3.1. Augmented Lagrangian method

Augmented Lagrangian methods are a specific category of algorithms developed for tackling constrained optimization problems. They share commonalities with penalty methods in their approach of transforming constrained optimization challenges into a sequence of unconstrained problems, supplemented with a penalty term incorporated into the objective function. However, their introduction of an additional term strategically designed to emulate a Lagrange multiplier sets augmented Lagrangian methods apart. While the augmented Lagrangian method is closely related to the technique of Lagrange multipliers, it is not identical. Notably, this methodology is exceptionally valuable when presenting the concept of proposed compactness in a broader context. This concept revolves around the reduction of data redundancy within the blockchain.

The fuzzy augmented Lagrangian function $L (x, \lambda)$ can be represented as:

$L (x, \lambda) = f(x) + \Sigma (\lambda_i * g_i(x)) + \Sigma (\mu_i * [g_i(x)]^{+})$ where

λ_i is the Lagrange multiplier associated with the i-th constraint.

μ_i is the fuzzy Lagrange multiplier associated with the i-th constraint.

[g_i(x)] ^+ represents the positive part of the constraint g_i(x), i.e., max (0, g_i(x)).

The Σ notation represents the summation of all constraint terms.

3.2. Data Redundancy Problem

Data redundancy in blockchain refers to the situation where the same or similar information is stored in multiple places within the blockchain network. This can occur due to the decentralized and distributed nature of blockchain systems, where multiple nodes store and validate the same data. While data redundancy might be beneficial in some cases for enhancing security and resilience but can lead to inefficiencies, increased storage requirements, and potentially compromise the overall performance of the blockchain system.

The presence of data redundancy within a blockchain system can give rise to various adverse consequences, including the escalation of storage requirements, network latency, reduced throughput, elevated energy consumption, diminished packet delivery ratio, blockchain bloat, and extended processing times. While many strategies are available to mitigate these challenges, our investigation has unveiled an innovative solution: integrating compact blocks. By adopting this approach, we aim to surmount these contemporary issues effectively. Our comprehensive performance analysis demonstrates that our proposed FALORR excels in all aspects, encompassing memory utilization and security, and introduces significant enhancements across the board.

3.3. Compact blocks

Compact blocks are the protocols that can transmit the blocks' information between the nodes that make up the network. Compact blocks can help reduce the bandwidth requirements of the Bitcoin network by transmitting only the essential information about each block. The Blockchain network has a high volume of information traffic because it has many nodes, receives many transactions per second, and generates blocks containing a lot of data every 10 minutes. The introduction of the Compact Block Relay protocol marks a noteworthy advancement in the field of blockchain technology. [32]

3.3.1. Working of Compact Blocks

The first step involves block generation, where miners create a valid block adhering to consensus rules. Referred to as a compact block, it contains all standard block information such as nonce, timestamp, hash, and Merkle root encompassing the complete transaction set. Along with these, it will have a list of short transaction identifiers. During this phase, the block generation process remains unchanged, without any modifications. The full transaction data is only transmitted if a node specifically requests it. The second step is transmitting this data, showcasing the novelty of compact blocks. Every node within the Blockchain's network possesses a dedicated space known as a mempool [33] [34]. This repository houses pending transactions awaiting processing and is ubiquitous across all nodes. This setup enables us to infer a significant portion of the transactions present in the recently formed block, as each node's mempool contains all corresponding transaction hashes. Fig 4 shows the compact block structure.

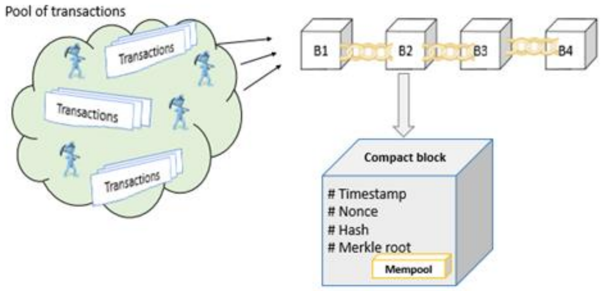


Fig 4. Compact block structure

Integrating compact blocks and mempool streamlines data transmission within the network and fundamentally addresses the challenge of memory consumption. This duality of benefits expedited data communication and reduced memory demands represents a pivotal step toward enhancing the overall performance and scalability of blockchain systems. In our arrangement, the hash values of encrypted transaction records are stored in the blockchain, and the relevant index set is stored in the compact blocks, which provides a new idea to solve the redundancy problem. Compact blocks are over ten times smaller than standard blocks, resulting in delivery time enhancements ranging from 0% to 20%. [35] [36]

4. Proposed Model – FALORR

In response to the pressing challenges posed by data redundancy in blockchain systems, we present a novel and powerful solution in the form of FALORR.

4.1. Design goals

Our goal is to address the problem of redundancy by enhancing the compactness of the blockchain. We have coined our innovative approach as "Compactness" which introduces a novel concept termed "Fuzzy Augmented Lagrangian-based Redundancy Reductant", FALORR in short form. This approach seeks to effectively minimize redundancy within the blockchain system. By leveraging this thorough understanding of the prior research landscape, we developed a carefully tailored approach that significantly enhances data integrity within the context of blockchain technology. Our proposed framework employs Fuzzy Augmented Lagrangian Optimization in conjunction with the utilization of compact blocks. This combination harnesses the power of advanced optimization techniques alongside the efficiency gains achieved through compact blocks. We assure FALORR is significant in Redundancy Minimization, Enhanced Efficiency, and Compatibility in facilitating optimizing storage space, streamlining data storage, and easy adoption respectively.

4.2. Workflow of the scheme

The scheme operates through a straightforward sequence of four stages:

4.2.1. Initialization Stage – Miners conveying the blocks

During the Initialization Stage, miners communicate and share newly created blocks on the blockchain network. This process involves the distribution of block data among miners for verification and eventual inclusion in the blockchain ledger.

4.2.2. Loading Stage - Storing Transactions in Blocks

During the Loading Stage, transactions are grouped and stored within blocks in the blockchain. This step involves organizing and structuring transaction data before it's added to the block, ensuring efficient data storage and subsequent validation.

4.2.3. Allotment Stage - Incorporating Compact Blocks

In the Allotment Stage, compact blocks are integrated, allocating space within the blockchain for streamlined data representation. This phase optimizes storage by reducing redundancy and enhancing overall transaction efficiency.

4.2.4. Management Stage - Ledger-Based Transaction Handling

In the Management Stage, transactions are processed and managed based on the ledger's structure. This step involves validating and recording transactions within the Blockchain's ledger, ensuring data integrity and consistency.

Initiation entails miners transmitting blocks to the blockchain. Transactions are stored conventionally in the blockchain, which is a phase we label as the loading stage. Subsequently, in the allotment stage, compact blocks are introduced, populated with hashes of redundant data, and identified through a fuzzy augmented Lagrangian optimization algorithm. Finally, similar to regular blocks, transactions within compact blocks are also ledger-managed. The Fig 5 illustrates the workflow.

The compact block effectively addresses the issue of redundant blocks by storing them in a compressed format. When the user issues a get-data instruction, the sender responds with a compact block containing a transaction summary of the entire block. The receiver can then swiftly request transaction verification and assess non-redundant data instead of verifying all hashes. This process ensures the rapid acquisition of essential information within moments.

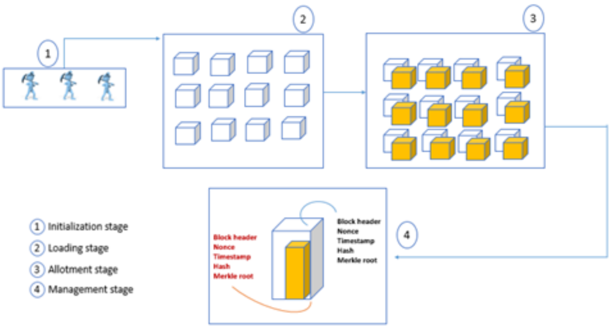


Fig 5. Workflow of the scheme

4.3. Scheme details

Our novel approach, Compactness, is achieved using a technique called Fuzzy Augmented Lagrangian Optimization-based Redundancy Reductant, abbreviated as FALORR. We proceed to elaborate on the intricacies of this model in the subsequent explanation.

Data redundancy is one of the impediments that is naturally inherited by distributed ledger technology. Fuzzy Augmented Lagrangian Optimization based Redundancy Reductant module is introduced here to reduce the data redundancy in the proposed blockchain environment. The Fuzzy logic part labels the ledger block into three categories based on the replications. The schemed Redundancy Labels (RL) are Rare, Frequent, and Plenty based on the number of replications of the same block in the overall blockchain. The RL tagging process operates based on the X-OR-based hash comparison of the blocks, thus using a negligible computational resource.

In the suggested FALORR module, every ledger is treated as a set represented as λ. Thereby a blockchain contains many ledger copies such as $\{\lambda_1, \lambda_2, \lambda_3 \dots . \lambda_n\}$, where n is the maximum number of ledgers in the blockchain. Every ledger can have several associated blocks as represented in Equation 1.

$$\lambda_i = \{bi_1, bi_2 \cdots bi_m\} \qquad \text{Equation (1)}$$

where bi_1, bi_2 ... are the blocks belonging to ledger λ_i, and bi_m is the total number of blocks in the same ledger

Thus, the entire blockchain is represented as a superset L as in Equation 2.

$$L = \{\lambda_1 = \{b1_1, b1_2 \cdots b1_m\}, \lambda_2 = \{b2_1, b2_2 \cdots b2_m\} \dots \lambda_n = \{bn_1, bn_2 \cdots bn_m\}\}$$

Equation (2)

The set representation simplifies the redundancy labelling process since the entire operation is performed over a single set. An illustration of the FALORR blockchain is given in Fig 6.

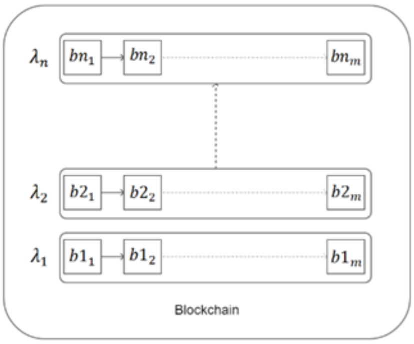


Fig 6. FALORR Blockchain Representation

```
Algorithm 1: FALORR Redundancy Labelling Algorithm
Input: $L$
Output: Redundant Block Set $R$ with Labels

Step 1: Let $R$ be the redundant block label initialized as $R = \emptyset$
Step 2: Load FALORR Blockchain set $L$
Step 3: Let $\gamma_{bx_y}$ be the redundant count of $y^{th}$ block of Ledger $\lambda_x$
Step 4: $\forall i = 1 \rightarrow n \coloneqq \forall j = 1 \rightarrow bi_m \coloneqq \forall k = 1 \rightarrow n \coloneqq \forall l = 1 \rightarrow bk_m$
Step 5: if $\left(i \neq k \ \&\left(Hash\left(bi_j\right) \oplus Hash\ (bk_l) = 0\right)\right)$
then Increment $\gamma_{bi_j}$ if $bi_j \in R$, else Append $bi_j$ to $R$ with $\gamma_{bi_j} = 0$
Step 6: Let $N_R$ be the number of elements in Redundant set $R$
Step 7: $\forall i = 1 \rightarrow N_R \coloneqq$ Determine $RL$ for $i^{th}$ member using Equation 3
Step 8: Return $R$
```

The redundant label-determining equation is as follows

$$RL = \begin{cases} Rare\ if\ \gamma_{bx_y} < \frac{N_R}{4} \\ Frequent\ if\ \frac{N_R}{4} \leq \gamma_{bx_y} < \frac{N_R}{2} \\ Plenty\ if\ \gamma_{bx_y} \geq \frac{N_R}{2} \end{cases}$$

Equation (3)

where N_R is the number of elements of redundant set R

The augmented Lagrangian optimization determines the number of redundant blocks that can be compressed and stored as compact blocks. The proposed FALORR method follows the Compact Block Relay protocol, thus seamlessly incorporating compact blocks in a ledger λ_x seamlessly. Since a compact block contains only the hash value of the entire transaction information of the block instead of having the entire data, the memory requirement will be lesser than a regular block. A ledger with regular and compact blocks is illustrated in Fig 7.

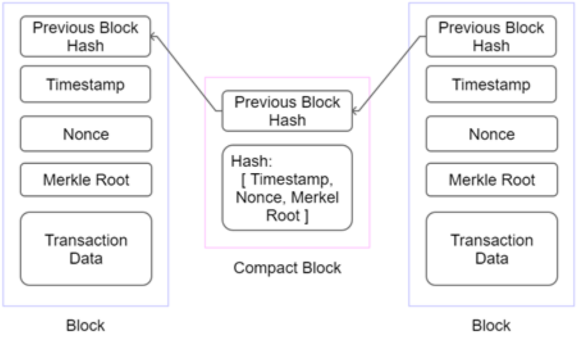


Fig 7. Ledger with Compact Blocks

The incorporation of Compact blocks into a regular blockchain architecture enables a faster and more efficient way of communicating data among the network as well as reduces the memory requirement.

The Augmented Lagrangian algorithm operates based on the successive minimization procedure This is formulated as Equation 4 for the successive minimization of Augmented Lagrangian A_A with respect to A_x and A_λ

$$min\left\{f(A_x) + \sum_{i \in A_\varepsilon} A_{\lambda_i} A_{c_i}(A_x) + \frac{\sum_{i \in A_\varepsilon} A_{v_i} A_{c_i}{}^2(A_x)}{2} : l \leq A_x \leq A_u\right\}$$

Equation (4)

The value if A_x is declared as in equation 5

$$A_x = \begin{cases} 0\ if\ RL = Rare \\ {}^1/_3\ if\ RL = Frequent \\ {}^2/_3\ if\ RL = Plenty \end{cases} \quad \text{Equation (5)}$$

For every block that attains the A_A value is 1 will be compressed to the compact blocks and for blocks with the A_A values are 0 will be maintained as regular blocks in the FALORR blockchain model. The integration of Fuzzy and Augmented Lagrangian methodologies and the compact blocks concept ensures the compactness of the proposed blockchain model.

5. Experimental Results and Analysis

Caliper serves as a performance benchmark framework within the realm of blockchain technology, and it stands as one of the projects under the umbrella of Hyperledger, an initiative managed by The Linux Foundation [37]. Since it integrates well with distributed ledger technology, the blockchain network is conducted on the Hyperledger Caliper, which is a programmed performance assessment framework [38]. Hyperledger Caliper is a leading open-source, general-purpose blockchain structure built for enterprises. Since Hyperledger does not require mining, it does not require strong hardware support nor consume resources, and its allowable transactions per minute are much greater than Ethereum. [17] Through rigorous experimentation and analysis, we have observed substantial improvements in the verification and integrity of transactions within our blockchain-based system. These findings underscore the effectiveness and viability of our proposed approach compared to the methodologies outlined in the existing papers. Our work builds upon prior research and advances the field by providing a holistic solution addressing critical blockchain data integrity challenges. To exhibit the strength of our proposed framework, we carried out a thorough examination of the parameters that share an identical timestamp. The outcomes of this analysis were visually presented through Table 1 accompanied by pertinent graphs. Evaluating the existing schemes and proposed FALORR against the selected parameters for comparison has yielded distinct outcomes. The parameters leveraged for the proposed work with the findings are:

5.1. Improved Throughput

FALORR aims to boost the efficiency of the blockchain system by minimizing the processing burden linked to repetitive data. This improvement is evident in the comparative graph, where the reading prominently registers at 31781 kbps at the timestamp of 5.

5.2. End-to-end delay

End-to-end delay pertains to the duration required for data to traverse a network from its origin to its destination. FALORR accomplishes this task notably faster, completing it in just 281 milliseconds with a timestamp reading of 5.

5.3. Average processing time

In terms of average processing time for data transactions, the FALORR scheme demonstrates remarkable performance, particularly when juxtaposed with other established methods that we included in our comparative assessment. Our findings reveal that FALORR achieves an outstanding result of 1483 milliseconds, signifying its superiority in this specific parameter.

5.4. Energy Efficiency

FALORR is anticipated to play a role in reducing energy usage, fostering sustainability, and curtailing the ecological footprint of the blockchain network. Despite the energy readings being closely matched with other alternatives, our proposed FALORR exhibits lower energy consumption, registering 225 joules.

5.5. Average authentication time

The average authentication time, a critical requirement for every transaction within the blockchain network, holds significant importance. Fortunately, FALORR achieves a commendable authentication time of 67 milliseconds when the timestamp is set at 5.

5.6. Packet delivery ratio or Latency

The packet delivery time or latency is the time from when the first bit leaves the transmitter until the last is received. The scheme aims to minimize network latency by transmitting and processing only essential data, thereby accelerating transaction confirmation times. The observed packet delivery ratio from our proposed FALORR stands at 99.42 kbps.

5.7. Robust Security

While achieving data reduction, FALORR remains committed to upholding the security and integrity of the blockchain. This is accomplished by retaining adequate redundancy for fault tolerance and thwarting potential vulnerabilities. The results underscore the effectiveness of the proposed scheme, showcasing an impressive reading of 99.44 kbps.

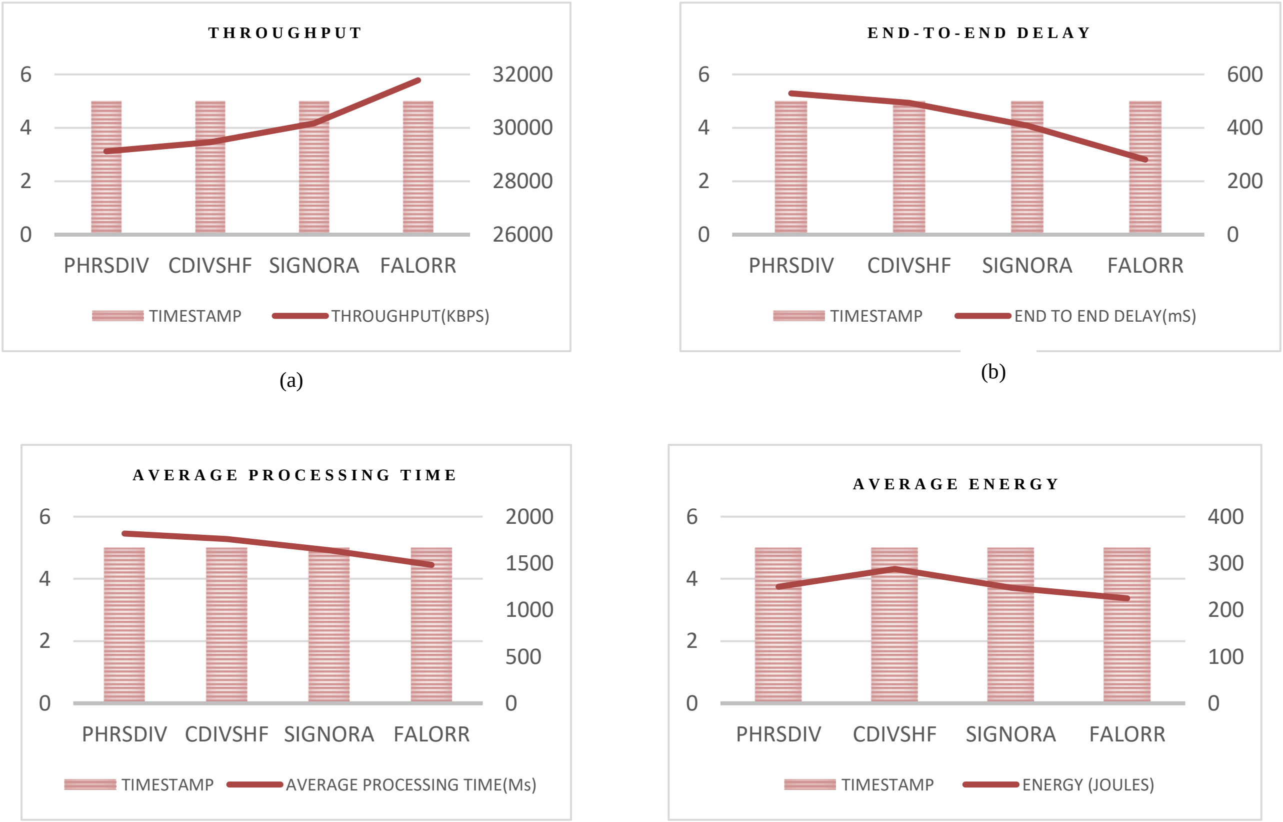
5.8. Memory

Memory plays a pivotal role in effectively storing data. In the realm of blockchain technology, a significant focus of research has centered around scalability, aiming to enhance the system's capacity to handle growing demands. With this concern in mind, we dedicated substantial effort to devising a meticulous scheme. The outcome of our efforts is noteworthy as our proposed FALORR demonstrates a commendable memory usage of 113 megabytes (MB). This achievement stands out favorably in comparison to the memory utilization of other pre-existing schemes.

Table 1. The evaluation of the existing schemes and proposed FALORR against the selected parameters.

Parameters	Scheme			
	PHRSDIV	**CDIVSHF**	**SIGNORA**	**FALORR(proposed)**
Timestamp	5	5	5	5
Throughput (kbps)	29121	29465	30169	31781
End-to-end delay(ms)	529	494	408	281
Average processing time(ms)	1819	1760	1641	1483
Average Energy (Joules)	250	288	248	225
Average authentication (ms)	123	115	96	67
Packet delivery ratio (kbps)	89.22805	90.236565	93.929619	99.418365
Security(kbps)	97.63	98.77	98.98	99.44
Memory(MB)	128	121	131	113

Presented in Fig 8 are graphical depictions of the findings resulting from our comprehensive analysis. Each graphical representation vividly illustrates the pronounced superiority of our proposed FALORR scheme across all assessed parameters. It is important to underscore that this presentation of results does not diminish the significance of prior endeavors put forth by various authors. We intend to provide a comparative assessment of schemes based on the selected parameters.



(a)

(b)

(c)

(d)

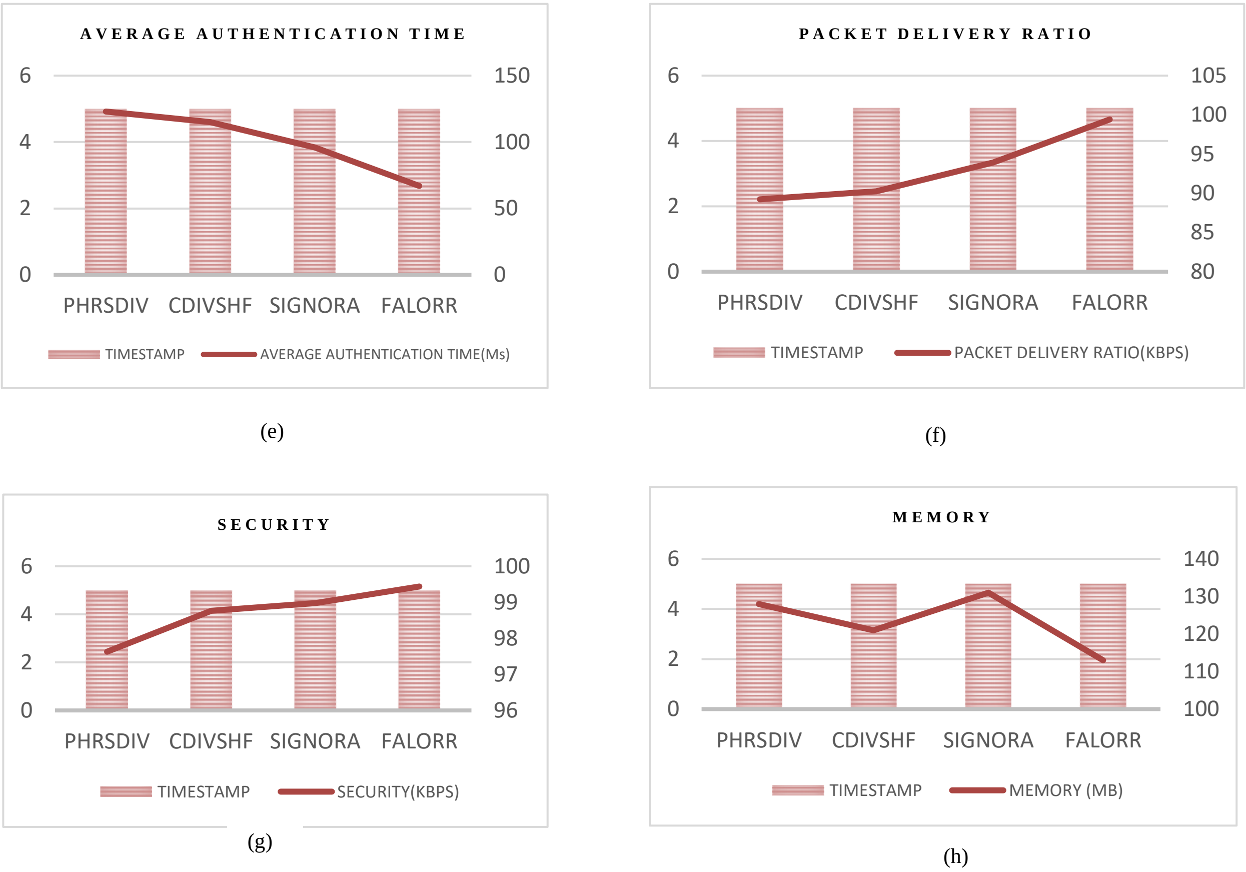


Fig 8. Graphical depictions of the findings resulting from our comprehensive analysis based on the selected parameters. (a) Throughput. (b) End-to-end delay. (c)Average processing time. (d)Average energy. (e)Average authentication time. (f) Packet delivery ratio. (g) Security. (h) Memory.

6. Performance Analysis

To establish a comprehensive context for comparing our proposed work, we meticulously analyzed three prominent existing research papers in the realm of blockchain-based data integrity. We delved deeply into the methodologies these papers employed and thoroughly grasped the underlying purposes of their respective approaches. We precisely crafted our work based on the insights gained from this analysis. The relevant research on encryption technology and blockchain technology related to the scheme is discussed, and a comparison table is given in Table 2.

The first scheme is “Blockchain-Based Personal Health Records Sharing Scheme with Data Integrity Verifiable” (PHRSDIV). In this paper Wang et al. [39] proposed an approach that involves the patient's generation and distribution of a private key tied to attributes for the user. This unique feature facilitates precise access control, eliminating the need for third-party involvement. Leveraging the decentralized and tamper-resistant nature of the blockchain, the scheme utilizes it to enhance the security of key management and distribution. Additionally, the blockchain stores

hash values of encrypted personal health records while the corresponding index set is retained within the smart contract. This setup empowers the recipient of personal health records to conveniently and swiftly verify the authenticity and integrity of encrypted data received from the cloud server.

The first scheme is “Blockchain-Based Personal Health Records Sharing Scheme with Data Integrity Verifiable” (PHRSDIV). In this paper Wang et al. [39] proposed an approach that involves the patient's generation and distribution of a private key tied to attributes for the user. This unique feature facilitates precise access control, eliminating the need for third-party involvement. Leveraging the decentralized and tamper-resistant nature of the blockchain, the scheme utilizes it to enhance the security of key management and distribution. Additionally, the blockchain stores hash values of encrypted personal health records while the corresponding index set is retained within the smart contract. This setup empowers the recipient of personal health records to conveniently and swiftly verify the authenticity and integrity of encrypted data received from the cloud server.

The second scheme is “Blockchain-Based Cloud Data

Integrity Verification Scheme with High Efficiency" (CDIVSHE), where Xie et al. [40] proposed a lattice signature algorithm designed to withstand quantum computing and introduce a cuckoo filter to streamline the computational workload during user verification stages. They integrated blockchain as a third-party auditing mechanism, substituting the conventional centralized audit and involving users, CSP, and blockchain as participants. The process entails utilizing the lattice signature algorithm for file signing at the user end, leveraging the cuckoo filter to streamline user verification, and implementing a blockchain network to log user-CSP interactions.

The third scheme is "A Blockchain-Based Framework for Dataflow Integrity Provisioning in an Untrusted Data Pipeline" (SIGNORA). Here, Oktian et al. [41] integrated the notion of a signature chain with the concept of blockchain receipts. In this scheme, participants in the process took alternating roles in generating signatures for the data they were actively handling. Subsequently, both the signatures and the hash of the data were immutably recorded on the blockchain. This method was implemented to enhance integrity assurance via blockchain receipts. The study's outcomes offer insights into the capacity of SIGNORA to establish dataflow integrity across various scenarios involving diverse data payload sizes while maintaining a manageable level of overhead. Furthermore, the research includes an examination of the expenses related to smart contract methods, along with a thorough exploration of various off-chain strategies that have been proposed to mitigate these costs.

Below is Table 2 and it provides a summary of the existing schemes and the proposed FALOR

Table 2. Scheme comparison with the existing scheme

Scheme	Algorithm	Location to leverage	Set-up	Participants	Tool used
PHRSDIV	Searchable symmetric and attribute-based encryption	Ethereum – smart contracts	Personal health record	Patient, user, cloud server	Remix
CDIVSHE	Lattice Signature Algorithm	Cuckoo filter	The unreliable problem of TPA	CSP, users, blockchain	Hyper ledger Fabric
SIGNORA	Chain of signatures	Smart contracts	Untrusted data pipeline	Trusted validator, IoT devices, manager	Go programming
FALORR-proposed	Fuzzy Augmented Lagrangian optimization	Compact block	Transactions	Sender, receiver, merkle tree	Hyper ledger Caliper

We undertook a functional comparison grounded in specific criteria, encompassing the assessment of the proposed concept's resilience against tampering and its capacity to navigate various constraints successfully. Of paramount importance is the determination of whether the suggested scheme inherently embodies a fundamental attribute of distributed networks—namely, the principle of "transparency"—across all operational facets. Noteworthy is the significance accorded to the user-friendliness of the proposed FALORR solution. Its intuitive and straightforward nature makes it a crucial point of comparison. Among the multifaceted aspects weighed a central focus is directed towards validating data integrity. This factor is a primary benchmark for selecting research papers that can be equitably compared. Throughout this rigorous evaluation process, our proposed FALORR approach consistently stands out as a superior contender across all dimensions. It emerges as a frontrunner, showcasing exceptional performance in every aspect. These findings are succinctly summarized in Table 3, with PHRSDIV assigned the representation of 1, CDIVSHE assigned the representation of 2, SIGNORA designated as 3, and our innovative FALORR method represented as 4. The markings 'Y' denotes yes and 'N' denotes no.

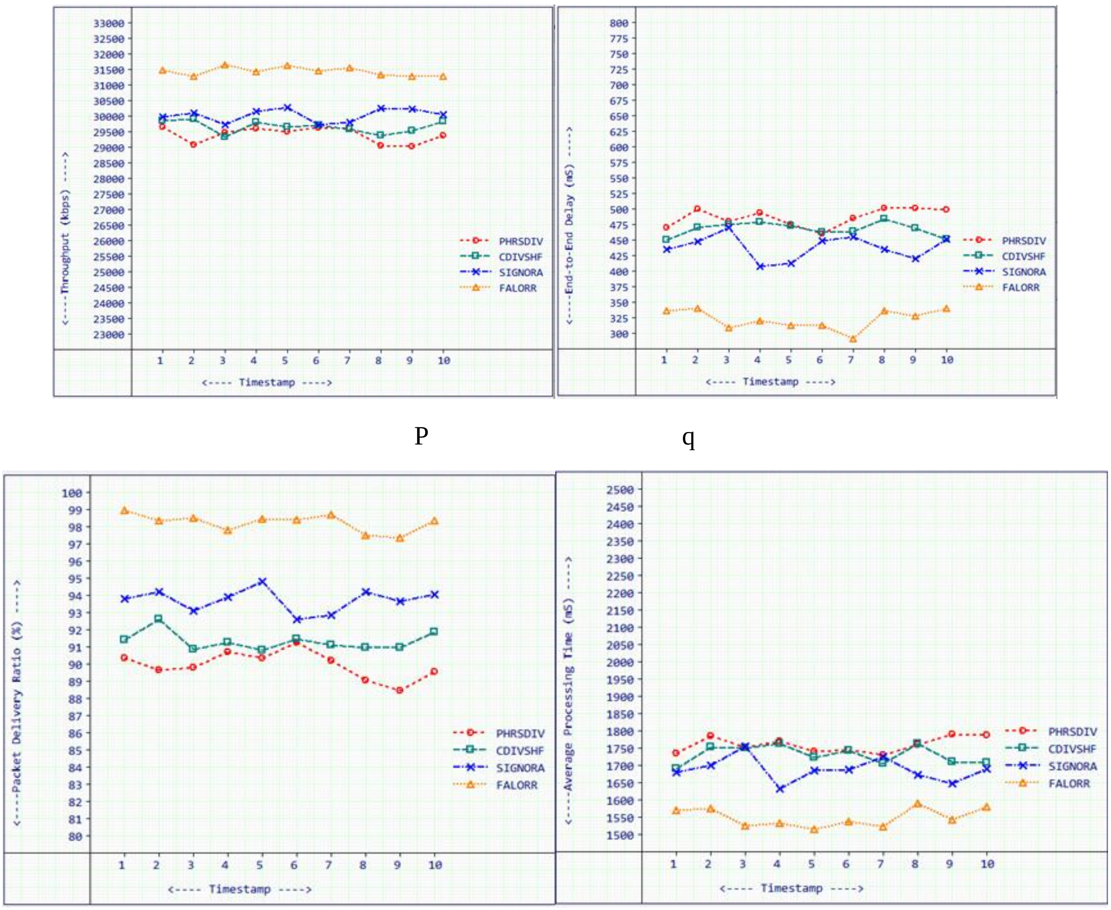
Table 3. Functional comparisons

Function	1	2	3	4
Tamper proof	Y	Y	Y	Y
Protection of private data	Y	Y	Y	Y
Data transparency	N	N	Y	Y

Ease of use	N	N	N	Y
Data integrity verification	Y	Y	Y	Y

The graphical representations presented in Fig 9 vividly illustrate the comprehensive performance evaluation of the FALORR scheme in comparison to existing schemes.

This evaluation was carried out over a time range spanning from 1 to 10 timestamps, and the graphs were dynamically generated by concurrently executing both the existing and proposed methods. Our approach to this analysis was characterized by meticulous attention to detail, involving a thorough examination of data through the implementation of the FALORR methodology. Our rigorous efforts yielded results that decisively favor the proposed FALORR method. A key contributing factor to this success is the implementation of compact blocks within the blockchain structure. These compact blocks have proven instrumental in effectively segregating redundant data transcriptions, thereby significantly reducing superfluous data within the blockchain network. The significance of this work extends to its potential applicability in crypto transactions involving Merkle tree generation. In such contexts, unpaired nodes are frequently duplicated to facilitate their transformation into paired nodes. By harnessing the capabilities of the proposed FALORR approach, the redundancy introduced by these duplicated nodes is substantially mitigated. This marks a valuable contribution that has the potential to greatly enhance the efficiency of crypto transactions. In essence, our efforts have resulted in a solution worthy of consideration for integration into various blockchain applications, particularly in scenarios requiring Merkle tree generation and optimization. The redundancy reduction achieved through the FALORR scheme promises practical benefits and enhanced performance within blockchain systems.

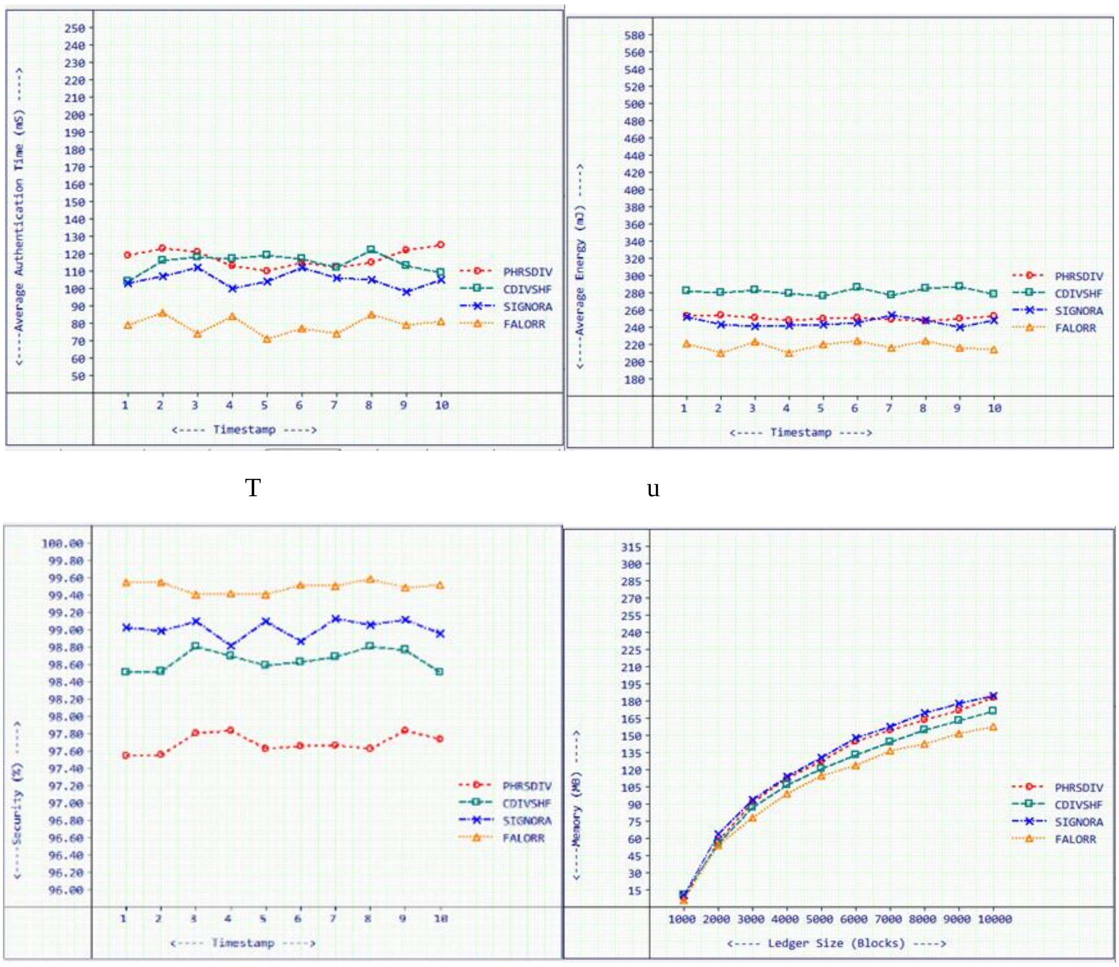


P

q

R

S



T u

(v) (w)

Fig 9. Performance evaluation of the FALORR scheme in comparison to existing schemes based on the selected parameters. (p) throughput. (q) End-to-end delay. (r)Average processing time. (s) Packet delivery ratio. (t)Average authentication time. (u) Average energy. (v) Security. (w) Memory.

We conducted an assessment of three distinct schemes, each yielding noteworthy findings. Our objective was not to undermine the significance of their discoveries. Instead, we aimed to evaluate a range of criteria, encompassing throughput time, processing duration, energy usage, authentication speed, end-to-end latency, packet delivery ratio, memory utilization, and security aspects. Through this all-encompassing analysis, our innovative FALORR scheme showcased remarkable performance, positioning it as the foremost candidate across the measured parameters.

7. Conclusion and Future Enhancement

A swift surge in the popularity of blockchain technology and the ongoing efforts to expand data within the Merkle tree structure, ensuring data integrity within this domain, has emerged as a timeless subject. Our paper introduces FALORR, an innovative data integrity verification scheme for blockchain designed to enhance efficiency through data compactness. By employing Fuzzy Augmented Lagrangian Optimization, we have successfully achieved this compactness while maintaining adaptability and precision in managing complex constraints. This advancement reduces redundancy, optimizes data storage and retrieval, and enhances transaction verification, thereby bolstering the security and dependability of blockchain technology. Our approach proves effective for compact blocks of a moderate size, but it is important to acknowledge that in the future, block sizes increase to accommodate higher transactions per second (tps). In turn, the compact blocks themselves will grow and can cause delays in data transmission. Our upcoming accomplishments will be focused on ensuring consistent throughput times for both smaller and larger compact blocks; addressing this challenge is our further contribution to the evolution of blockchain technology.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] David Berdika, Safa Otoum, Nikolas Schmidta, Dylan Portera, and Yaser Jararweh, “A Survey on Blockchain for

Information Systems Management and Security", doi: doi.org/10.1016/j.ipm.2020.10239.

[2] O. Ali, A. Jaradat, A. Kulakli, and A. Abuhalimeh, "A Comparative Study: Blockchain Technology Utilization Benefits, Challenges and Functionalities," IEEE Access, vol. 9, pp. 12730–12749, 2021, doi: 10.1109/ACCESS.2021.3050241.

[3] F. Lumineau, W. Wang, and O. Schilke, "Blockchain Governance—A New Way of Organizing Collaborations?," Organ. Sci., vol. 32, no. 2, pp. 500–521, Mar. 2021, doi: 10.1287/orsc.2020.1379.

[4] S. Das, S. Namasudra, and V. H. C. De Albuquerque, "Blockchain technology: fundamentals, applications, and challenges," in Blockchain Technology in e-Healthcare Management, S. Namasudra and V. H. C. De Albuquerque, Eds., Institution of Engineering and Technology, 2022, pp. 1–30. doi: 10.1049/PBHE048E_ch1.

[5] M. E. Khatib, F. Beshwari, M. Beshwari, and A. Beshwari, "The Impact of Blockchain on Project Management." ICIC International 学会, 2021. doi: 10.24507/icicel.15.05.467.

[6] S. M. Idrees, M. Nowostawski, R. Jameel, and A. K. Mourya, "Security Aspects of Blockchain Technology Intended for Industrial Applications," Electronics, vol. 10, no. 8, p. 951, Apr. 2021, doi: 10.3390/electronics10080951.

[7] G. S. Sajja, K. P. Rane, K. Phasinam, T. Kassanuk, E. Okoronkwo, and P. Prabhu, "Towards applicability of blockchain in agriculture sector," Mater. Today Proc., vol. 80, pp. 3705–3708, 2023, doi: 10.1016/j.matpr.2021.07.366.

[8] M. Javaid, A. Haleem, R. Pratap Singh, S. Khan, and R. Suman, "Blockchain technology applications for Industry 4.0: A literature-based review," Blockchain Res. Appl., vol. 2, no. 4, p. 100027, Dec. 2021, doi: 10.1016/j.bcra.2021.100027.

[9] G. Gad, D. T. Mosa, L. Abualigah, and A. A. Abohany, "Emerging Trends in Blockchain Technology and Applications: A Review and Outlook," J. King Saud Univ. - Comput. Inf. Sci., vol. 34, no. 9, pp. 6719–6742, Oct. 2022, doi: 10.1016/j.jksuci.2022.03.007.

[10] *Satoshi* Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System,"

[11] H. Liu, X. Luo, H. Liu, and X. Xia, "Merkle Tree: A Fundamental Component of Blockchains," in 2021 International Conference on Electronic Information Engineering and Computer Science (EIECS), Changchun, China: IEEE, Sep. 2021, pp. 556–561. doi: 10.1109/EIECS53707.2021.9588047.

[12] Z. Liu, L. Ren, Y. Feng, S. Wang, and J. Wei, "Data Integrity Audit Scheme Based on Quad Merkle Tree and Blockchain," IEEE Access, vol. 11, pp. 59263–59273, 2023, doi: 10.1109/ACCESS.2023.3240066.

[13] Tan Tao, "Research on Pow Scheme and Blockchain Security Technology Based on Merkel Tree," vol. 3, no. 4, 2021.

[14] R. Johari, V. Kumar, K. Gupta, and D. P. Vidyarthi, "BLOSOM: BLOckchain technology for Security Of Medical records," ICT Express, vol. 8, no. 1, pp. 56–60, Mar. 2022, doi: 10.1016/j.icte.2021.06.002.

[15] J. Misic, V. B. Misic, and X. Chang, "On the Benefits of Compact Blocks in Bitcoin," in ICC 2020 - 2020 IEEE International Conference on Communications (ICC), Dublin, Ireland: IEEE, Jun. 2020, pp. 1–6. doi: 10.1109/ICC40277.2020.9149418.

[16] R. Kalis and A. Belloum, "Validating Data Integrity with Blockchain," in 2018 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Nicosia: IEEE, Dec. 2018, pp. 272–277. doi: 10.1109/CloudCom2018.2018.00060.

[17] W. Choi and J. W.-K. Hong, "Performance Evaluation of Ethereum Private and Testnet Networks Using Hyperledger Caliper," in 2021 22nd Asia-Pacific Network Operations and Management Symposium (APNOMS), Tainan, Taiwan: IEEE, Sep. 2021, pp. 325–329. doi: 10.23919/APNOMS52696.2021.9562684.

[18] M. S. Rahman, M. A. P. Chamikara, I. Khalil, and A. Bouras, "Blockchain-of-blockchains: An interoperable blockchain platform for ensuring IoT data integrity in smart city," J. Ind. Inf. Integr., vol. 30, p. 100408, Nov. 2022, doi: 10.1016/j.jii.2022.100408.

[19] L. Hang and D.-H. Kim, "Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity," Sensors, vol. 19, no. 10, p. 2228, May 2019, doi: 10.3390/s19102228.

[20] T. Alam, "Blockchain-Based Big Data Integrity Service Framework for IoT Devices Data Processing in Smart Cities," SSRN Electron. J., 2021, doi: 10.2139/ssrn.3869042.

[21] S. Hariharasitaraman and S. P. Balakannan, "A dynamic data security mechanism based on position aware Merkle tree for health rehabilitation services over cloud," J. Ambient Intell. Humaniz. Comput., Jul. 2019, doi: 10.1007/s12652-019-01412-0.

[22] P. Mohan, Mohamed Asfak R., and A. Gladston, "Merkle Tree and Blockchain-Based Cloud Data Auditing:," Int. J. Cloud Appl. Comput., vol. 10, no. 3, pp. 54–66, Jul. 2020, doi: 10.4018/IJCAC.2020070103.

[23] Mizrahi, N. Koren, and O. Rottenstreich, "Optimizing Merkle Proof Size for Blockchain Transactions," in 2021 International Conference on COMmunication Systems &

NETworkS (COMSNETS), Bangalore, India: IEEE, Jan. 2021, pp. 299–307. doi: 10.1109/COMSNETS51098.2021.9352820.

[24] G. Zhang, G. Wang, C.-H. Chen, X. Cao, Y. Zhang, and P. Zheng, “Augmented Lagrangian coordination for energy-optimal allocation of smart manufacturing services,” Robot. Comput.-Integr. Manuf., vol. 71, p. 102161, Oct. 2021, doi: 10.1016/j.rcim.2021.102161.

[25] G. Zhang, Y. Zhang, R. Y. Zhong, and Y. Wu, “Extending augmented Lagrangian coordination for the optimal configuration of cloud-based smart manufacturing services with production capacity constraint,” Robot. Comput.-Integr. Manuf., vol. 58, pp. 21–32, Aug. 2019, doi: 10.1016/j.rcim.2019.01.009.

[26] L. Dhavamani and P. Prem Priya, “Energy-efficient and privacy-preserving approach for INTERNET OF THINGS nodes using a novel hybrid fuzzy water cycle and evaporation strategy and matrix-based Rivest–Shamir–Adleman encryption algorithm,” Concurr. Comput. Pract. Exp., vol. 34, no. 27, p. e7336, Dec. 2022, doi: 10.1002/cpe.7336.

[27] G. Habib, S. Sharma, S. Ibrahim, I. Ahmad, S. Qureshi, and M. Ishfaq, “Blockchain Technology: Benefits, Challenges, Applications, and Integration of Blockchain Technology with Cloud Computing,” Future Internet, vol. 14, no. 11, p. 341, Nov. 2022, doi: 10.3390/fi14110341.

[28] M. Hashemi Joo, Y. Nishikawa, and K. Dandapani, “Cryptocurrency, a successful application of blockchain technology,” Manag. Finance, vol. 46, no. 6, pp. 715–733, Aug. 2019, doi: 10.1108/MF-09-2018-0451.

[29] J. Bao, D. He, M. Luo, and K.-K. R. Choo, “A Survey of Blockchain Applications in the Energy Sector,” IEEE Syst. J., vol. 15, no. 3, pp. 3370–3381, Sep. 2021, doi: 10.1109/JSYST.2020.2998791.

[30] F. A. Sunny et al., “A Systematic Review of Blockchain Applications,” IEEE Access, vol. 10, pp. 59155–59177, 2022, doi: 10.1109/ACCESS.2022.3179690.

[31] I. Ozdemir, I. M. Ar, and I. Erol, “Assessment of blockchain applications in travel and tourism industry,” Qual. Quant., vol. 54, no. 5–6, pp. 1549–1563, Dec. 2020, doi: 10.1007/s11135-019-00901-w.

[32] J. Misic, V. B. Misic, and X. Chang, “Performance of Bitcoin Network With Synchronizing Nodes and a Mix of Regular and Compact Blocks,” IEEE Trans. Netw. Sci. Eng., vol. 7, no. 4, pp. 3135–3147, Oct. 2020, doi: 10.1109/TNSE.2020.3017453.

[33] M. Saad et al., “Exploring the Attack Surface of Blockchain: A Comprehensive Survey,” IEEE Commun. Surv. Tutor., vol. 22, no. 3, pp. 1977–2008, 2020, doi: 10.1109/COMST.2020.2975999.

[34] Manuskin, M. Mirkin, and I. Eyal, “Ostraka: Secure Blockchain Scaling by Node Sharding,” in 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Genoa, Italy: IEEE, Sep. 2020, pp. 397–406. doi: 10.1109/EuroSPW51379.2020.00060.

[35] L. Zhang, T. Wang, and S. C. Liew, “Speeding up block propagation in Bitcoin network: Uncoded and coded designs,” Comput. Netw., vol.

[36] 206, p. 108791, Apr. 2022, doi: 10.1016/j.comnet.2022.108791.

[37] “What is a Compact Block?" [Online]. Available: https://academy.bit2me.com/en/que-son-compact-block/

[38] “Hyperledger Caliper A performance benchmark framework for blockchain." [Online]. Available: https://events19.linuxfoundation.cn/wp-content/uploads/2017/11/Hyperledger-Caliper-A-Performance-Benchmark-Framework-for-Multiple-DLTs_Haojun-Zhou.pdf

[39] S. Aggarwal and N. Kumar, “Hyperledger,” in Advances in Computers, Elsevier, 2021, pp. 323–343. doi: 10.1016/bs.adcom.2020.08.016.

[40] S. Wang, D. Zhang, and Y. Zhang, “Blockchain-Based Personal Health Records Sharing Scheme with Data Integrity Verifiable,” IEEE Access, vol. 7, pp. 102887–102901, 2019, doi: 10.1109/ACCESS.2019.2931531.

[41] G. Xie, Y. Liu, G. Xin, and Q. Yang, “Blockchain-Based Cloud Data Integrity Verification Scheme with High Efficiency,” Secur. Commun. Netw., vol. 2021, pp. 1–15, Apr. 2021, doi: 10.1155/2021/9921209.

[42] Y. E. Oktian, S. Heo, and H. Kim, “SIGNORA: A Blockchain-Based Framework for Dataflow Integrity Provisioning in an Untrusted Data Pipeline,” IEEE Access, vol. 10, pp. 89714–89731, 2022, doi: 10.1109/ACCESS.2022.3199878.

[43] Mujawar, S. S. ., & Bhaladhare, P. R. . (2023). Effective Feature Selection Methods for User Sentiment Analysis using Machine Learning. International Journal on Recent and Innovation Trends in Computing and Communication, 11(3s), 37–45. https://doi.org/10.17762/ijritcc.v11i3s.6153

[44] Robert Roberts, Daniel Taylor, Juan Herrera, Juan Castro, Mette Christensen. Integrating Virtual Reality and Machine Learning in Education. Kuwait Journal of Machine Learning, 2(1). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/175

[45] Kumar, S.A.S., Naveen, R., Dhabliya, D., Shankar, B.M., Rajesh, B.N. Electronic currency note sterilizer machine (2020) Materials Today: Proceedings, 37 (Part 2), pp. 1442-1444.