International Journal of Applied Mathematics

Volume 38 No. 8s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

A HYPERGRAPH-ENHANCED CONSENSUS WITH SEMANTIC-AWARE GRADIENT-DRIVEN GOSSIP PROTOCOL FOR HIGH-PERFORMANCE BLOCKCHAIN NETWORK

***[1]Ravindra Janardan Lawande,[2]Sudhir Bapurao Lande,[3]Dr.Manisha Lande**

[1]Research Scholar,Department of Electronics and Telecommunication Engineering,College of Engineering Malegaon (Bk), Savitribai Phule Pune University, Malegaon Budruk, Maharashtra-413115,Maharashtra-413115, India,rjlawande25@gmail.com

[2]Professor,Department of Electronics and Telecommunication Engineering, Vidya Pratisthan's Kamalnayan Bajaj Institute of Engineering and Technology, Baramati, Maharashtra-413133, India. sudhir.lande@vpkbiet.org

[3]Associate Professor, Department of Mechanical Engineering Vidya Pratisthan's Kamalnayan Bajaj Institute of Engineering and Technology Baramati, Maharashtra-413133, India.,manisha.lande@vpkbiet.org

Abstract

Blockchain (BC) technology has gained much interest due to its inherent qualities of security, immutability and decentralization. Despite these benefits, standard BC networks continue to face a number of difficulties, including the vulnerability of conventional leader-based consensus procedures to targeted leader assaults, high block propagation delay, and duplicate network traffic. To overcome these shortcomings, this paper proposes a unique unified framework that combines a hyper-delegated-leader based byzantine fault tolerant (HD-LBFT) protocol with a semantic-aware gradient-driven gossip (SAGD-Gossip). HD-LBFT improves performance scalability by streamlining leader selection and communication through the use of Hypergraph structures. The SAGD-Gossip protocol replaces blind flooding with an intelligent on-demand mechanism that optimizes data transfer by routing pull requests among the effective channels in terms of semantic role, latency and criticality. This technique significantly lowers propagation delays and duplicate network broadcasts while maintaining data integrity among peers. Experimental evaluation indicates that the proposed model enhances BC performance in terms of transaction confirmation latency obtained at node 10. The proposed model achieved a lower latency of 0.25s, block propagation latency of 261.5712ms with a block size of 0.1 MB, and block reception latency attained 217.1126ms with a block size of 0.1 MB. The proposed techniques provide a scalable, high performance and secure decentralized BC network, making it suitable for use in other real-world applications such as distributed IoT systems, supply chain management and financial transactions.

Keywords: Consensus mechanism, hyper delegated, Byzantine fault tolerant, Semantic aware and Gossip protocol.

Received: August 11 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

1. Introduction

Blockchain (BC) technology is a revolutionary paradigm in the field of digital systems. It provides a decentralized, transparent, and secure infrastructure for managing digital transactions and data across industries such as supply chain management, finance, healthcare and the Internet of Things (IoT) [1]. Due to fundamental properties, including immutability, traceability and elimination of centralized intermediaries, BC has established itself as a key technology for contemporary digital ecosystems [2]. Blockchain facilitates the management of the extensive data generated by fifth-generation (5G) networks in a decentralized and secure manner [3]. The data layer, network layer, consensus layer, smart contract layer and application layer are the five functional layers that make up a typical BC system [4]. Peer-to-peer (P2P) communication is controlled by the network layer, which facilitates the propagation of blocks and transactions between distributed nodes. The basic mechanism for propagating information in this layer is whisper protocols, which ensure that each participating node has a synchronized and replicated copy of the distributed ledger [5]. Redundancy provides resilience and fault tolerance by reducing the chance of a single point of failure [6].

Many BC platforms use leader based byzantine fault tolerance (BFT) techniques, such as Practical byzantine fault tolerance (PBFT) in the consensus layer. In these systems, a single leader node coordinates block validation and consensus [7]. Emerging applications such as digital currency platforms, smart city, infrastructures, and industrial IoT (IIoT) systems that requires high scalability and real-time response suffer greatly from high latency and poor performance. Network performance issues such as excessive block receipt latency, transaction confirmation latency, block propagation latency and low performance measured in transactions per second (TPS) are caused by ineffective rumor communication combined with centralized leader based consensus [8]. Digital currency platforms, smart city infrastructure and IIoT systems are examples of latency-sensitive and large scale applications that suffer from high latency and poor performance [9]. To achieve demanding performance requirements in large-scale and real-time scenarios, improvements are needed at both the network and consensus levels. Rumor protocols can be improved to decrease needless contacts and boost data distribution efficiency, while consensus techniques can be improved to increase fault tolerance and speed up verification [10].

The BC speed is improved by the Solana turbine protocol, which splits blocks into smaller data packets and distributes in a tree like structure, in contrast to relay networks like Falcon and FIBRE that share blocks and transactions quickly [11]. Decentralized communication methods called gossip protocols involve random information exchange between nodes. Data is spread widely and reliably on P2P networks like Bit Torrent. The applications include distributed systems such as content delivery networks (CDNs) and distributed databases, as well as cloud platforms for load balancing and service discovery [12]. A local 5G operator (L5GO) ecosystem has significant problems that are being addressed by a BC-as-a-Service (BaaS) platform. Applications such as resource management (RM), fraud prevention (FP) and inter-operator agreements (IOA) are all well supported by BaaS systems. These processors

Received: August 11 2025

Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

deliver secure, high performance 5G operations by improving performance reliability and trust in building L5GO installations [13]. Network security is significantly enhanced by installing ultra-dense keys. BC makes it possible to manage 5G network resources, including edge computing, spectrum allocation, and network slicing in an auditable and transparent manner. For a variety of 5G applications, such as the Internet of Things and ultra-reliable low latency communications (URLLC), this management guarantees excellent performance and great dependability [14]. Key performance indicators in BC networks, including block propagation delay (BPD), block reception delay (BRD), transaction confirmation delay (TCL) and TPS, are improved consensus and rumor tactics are being promoted. BC performance improvements help with high-volume and latency sensitive applications [15].

Motivation and Problem Statement

The high performance data integrity and the implementation of decentralized applications all depend on effective and secure data propagation across BC networks. There are many problems with traditional BC networks, including excessive network traffic, increased propagation delay and wasteful resource consumption due to indiscriminate flooding in gossip-based protocols. These issues are limiting adoption in large-scale applications, including supply chains, financial services and the Internet of Things (IoT). However, this paper proposes a new framework that combines SAGD-Gossip and HD-LBFT consensus process to solve these problems. The following is a list of key contributions of the proposed system:

- To improve network performance, scalability and resistance to leader attacks, an HD-LBFT consensus protocol is proposed.
- To develop a SAGD-Gossip protocol that reduces block propagation time and eliminates duplicate network traffic.
- The suggested architecture satisfies system requirements by increasing block receive delay, transaction volume, and data throughput.

By combining sophisti0063ated consensus process with efficient data propagation techniques, this integrated strategy provides an intelligent, scalable and secure solution for BC networks.

The rest of the paper is structured as follows: A review of the literature on BC consensus and gossip protocols is given in Section 2, the proposed methodology is outlined in Section 3, experimental findings and analyses are covered in Section 4, and the study is concluded in Section 5.

Related work

Some of the recent related models are surveyed and explained in detail in the following section:

Poongodi et al. [16] suggested a BC network architecture based on 5G for an encrypted keyword search engine. By using a variety of access node points and network brokers, the suggested model enables the simulation of all connections between various users and mini-base stations. The simulation kernel's findings demonstrate that this study, when paired with a

Received: August 11 2025

Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

decentralized cloud orchestration network system based on blockchain. The limitations of this study were high deployment costs, limited infrastructure, and risks to privacy.

Rahman et al. [17] presented the BlockSD-5GNet design in order to enhance the security of a 5G network and take advantage of the combined benefits of BC, software defined networking (SDN), network function virtualization (NFV), and machine learning (ML). Data may be successfully sent using this model design both within and across the 5G network infrastructure planes. The present research analyses this design and shows how the proposed solution performs compared to baseline methods through an experimental evaluation performed in a simulation environment. Computational overhead and storage requirements were the main constraints of this study.

Balani et al. [18] developed a sidechaining approach based on ML, which makes use of an engine driven by a modified genetic algorithm. By dividing the underlying blockchain into sidechains, this engine seeks to preserve real decentralization while lowering the complexity of mining and the quantity of packets required for communication. The model was helpful for highly scalable blockchain systems since it compares with the latency and delay of a normal blockchain. This study faces restrictions, including scalability issues, security vulnerabilities, and high operational costs.

Mafakheri et al. [19] introduced a novel 5G roaming network architecture built on a smart contract-based permissioned blockchain platform. In addition to facilitating speedy payment reconciliation and lowering fraudulent transactions, the suggested model gives mobile network operators better visibility into the activity of their users within the visiting network. The technique and architecture of the suggested solution utilizing the hyperledger platform were also covered in this study. One of the main drawbacks was the scalability issues focused on in this study.

Chaudhary et al. [20] suggested a blockchain-based voting system that uses the interplanetary file system (IPFS) and 5G to enable voters to elect candidates in a way that is affordable, dependable, and secure. Additionally, the deployed smart contract was assessed and examined based on a number of performance metrics, including bit error rate, storage cost comparison with the conventional scheme, cost analysis for smart contract functions, gas consumption analysis for smart contract functions, and the number of voters. The drawbacks of that method were privacy concerns, smart contract vulnerabilities, and voter accessibility issues.

Haddad et al. [21] developed an efficient and secure authentication and key agreement (AKA) scheme and uniform handover (HO) protocol for 5G networks using blockchain. The experimental findings show that the suggested HO technique can ensure forward and backward secrecy and is safe and consistent. The limitations of this study including high energy consumption, scalability issues, signaling overhead, potential delays, and integration complexity.

Balakumar et al. [22] investigated a novel cooperative NOMA-based CCR for underlay spectrum sharing was examined in this study. By taking into account the secondary users (SU) and relay access modes on the secondary network, a cooperative NOMA technique was

Received: August 11 2025

Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

suggested. Using the MATLAB simulation, the suggested methods were evaluated in a variety of scenarios while taking different transmit power levels, power location coefficients, and lengths into account. Latency constraints, energy consumption, security risks, and management complexity are the drawbacks.

Fei et al. [23] introduced a BC–based 5G network operations management scheme (B5G-NFM) model to address the centralized vulnerabilities in the service based architecture (SBA). The system includes a BC middleware for decentralized NF certificate management, NF service discovery and privacy preserving access authorization. The evaluation showed increased operational efficiency, security and privacy however, the framework has some scalability issues in very thin prophet installations and computational overhead issues in high-traffic situations.

Zhan et al. [24] introduced a delegated randomization byzantine fault tolerance (DRBFT) to enhance the efficiency and reliability of a consensus procedure. To speed up transaction processing, the framework provides a random selection (RS) method. This reduces the number of nodes that occur in consciousness, while preserving unpredictability, randomness and importability. Although this method has been proven by analysis and instrumental evaluations, however, the framework has some limitations, such as high transaction loads and possible defaults in very large-scale networks.

Li et al. [25] examined the algorithm in federated BC situations and improved the consensus mechanism to overcome the shortcomings of the PBFT method, such as fixed node membership, low multi-node consensus performance, and single master node dependency. A hierarchical structure is introduced by the improved method to improve consensus performance and scalability. Compared with PBFT and RAFT, simulation findings showed improved data performance support for more nodes and reduced consensus latency and communication between nodes. Table 1 below shows the survey of existing models.

Table 1: Survey of existing models

Reference	**Year**	**Methodology**	Limitations
Poongodi et al. [16]	2022	BC+5G keyword search	High cost
Rahman et al. [17]	2024	BlockSD-5GNet design	Computational overhead
Balani et al. [18]	2022	side chaining approach based on ML,	High cost
Mafakheri et al. [19]	2021	Smart contract-based BC	Scalability issues
Chaudhary et al. [20]	2023	BC based IPFS	SC vulnerabilities

Received: August 11 2025

Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Haddad et al. [21]	2021	AKA+HO using BC	Lack of energy signaling and scalability issues
Balakumar et al. [22]	2024	cooperative NOMA-based CCR	High generalization
Fei et al. [23]	2025	B5G-NFM	Scalability issues, storage overhead
Zhan et al. [24]	2021	DRBFT	Large scale load issues
Li et al. [25]	2021	PBFT	Limited real-world deployment

Although the frameworks [16]-[25] face issues with scalability, high computational cost, and poor generalization. Advanced consensus and network methods have improved speed and reliability; however, there are still limitations to their utilization of resources and practical use.

2.1 Research gap and novelty

It is significant to highlight that current BC-based architectures have a number of drawbacks that restrict their applicability, as per the review of existing techniques presented in Table 1. Due to the high costs and computational overhead, 5G integrated BC systems [16], [17] are not suitable for widespread applications. Similarly, side-chain methods based on machine learning [18] had significant operational costs, while designs based on smart contracts [19] had scalability issues. In the BC-based IPFS paradigm [20], smart contract flaws compromised overall network security. Furthermore, methods such as cooperative NOMA-based CCR [22] required a lot of generalization, which made the less flexible in dynamic network situations. Consensus technologies such as PBFT [25] and DRBFT [24] had limited real–world implementation and problems with large loads, respectively. More complex models, including B5G-NFM [23], have also struggled with scalability and storage cost, in contrast to AKA+HO employing BC [21], which is energy signal-less and has scaling restrictions.

To overcome these issues, the proposed framework presents a hybrid blockchain design that optimizes consensus and data exchange practices. By strengthening the consensus system to prevent errors caused by deliberate attacks and insufficient fault tolerance, it improves security and scalability. At the same time, the proposed framework increases data delivery by using an intelligent and flexible communication approach that reduces unnecessary network traffic, reduces latency and generally increases performance. A high-performance resource-effective BC network that provides effective, affordable, and scalable solutions for next generation decentralized systems is the result of this comprehensive strategy.

Received: August 11 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Proposed Methodology

BC technology has recently gained huge attention from both academia and industry due to its intrinsic properties, such as data immutability and decentralization. The BC architecture consists of five layers: data, network, consensus, smart contract, and application. Among these, the network layer is the origin of decentralization in BC. It basically designates the networking mechanism between peers on the BC and controls data propagation throughout the network via gossip protocols. Multiple peer-to-peer transactions ensure that the data blocks generated by the consensus method are duplicated on other peers in ledger form. This redundancy eliminates single-point-of-failure issues and ensures data integrity. As a result, optimizing the gossip protocol used for data propagation at the network layer is a highly beneficial and necessary step towards increasing the BC overall communication performance. Furthermore, a strong consensus mechanism is necessary to support efficient data dissemination, as it has a direct impact on transaction validation speed and system reliability. Therefore, this study intends to develop an enhanced consensus mechanism integrated with an optimized gossip protocol to improve blockchain performance in terms of latency, delay, and throughput. The consensus mechanism, known as the HD-LBFT protocol, is introduced in this study to create high-throughput, scalable, and secure decentralized BC networks. Figure 1 illustrates the workflow of the proposed methodology.

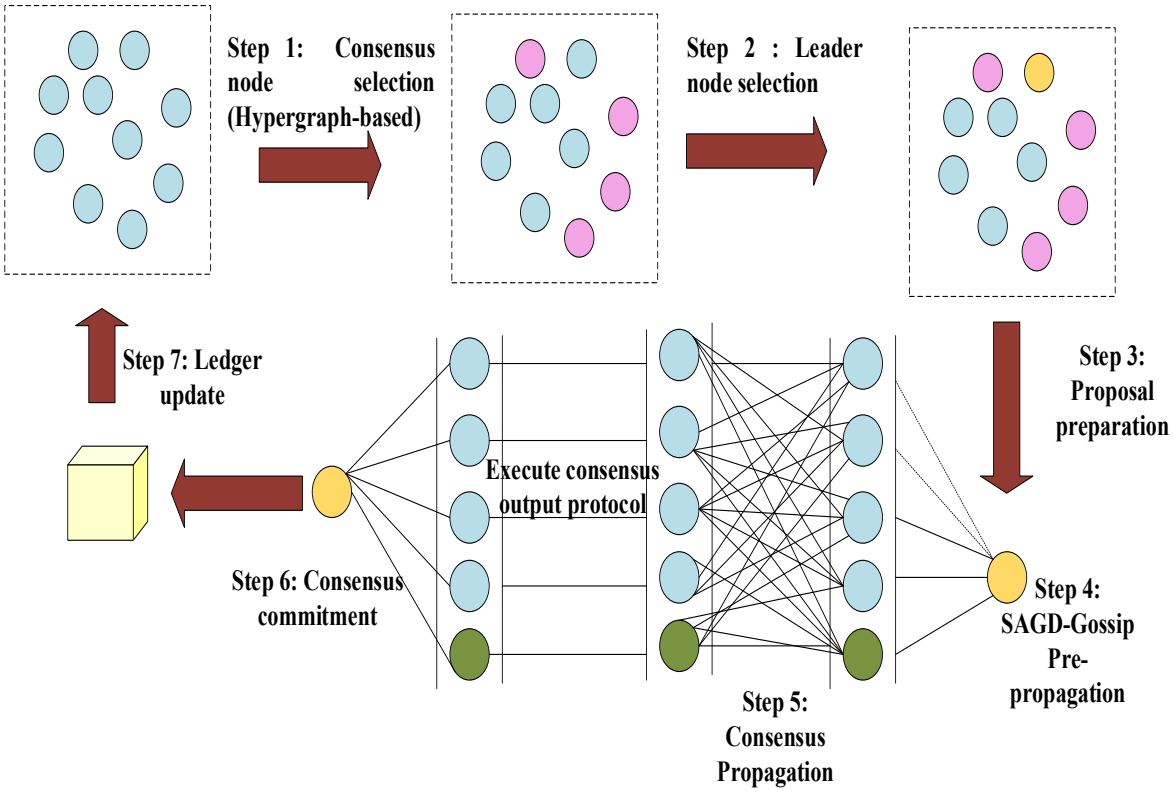

Figure 1: Work flow of proposed methodology

The proposed HD-LBFT protocol reorganizes the communication and leader-selection procedure by employing the mathematical structures of a Hypergraph to enhance the star-topology communication models of conventional leader-based BFT protocols. This creates a

Received: August 11 2025

Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

BC system that is more robust against targeted leader attacks, more efficient in its communication, and integrally more decentralized. In addition, the SAGD-Gossip protocol is designed to decentralize the dissemination of information as efficiently as possible. By using metrics like semantic role, latency, and criticality, the optimized gossip protocol determines the best channels to send data pull requests. The SAGD-Gossip algorithm drastically cuts down on propagation latency and redundant network traffic by substituting an intelligent, on-demand pull mechanism for random flooding.

3.1 Hyper Delegated-Leader based Byzantine fault Tolerant of Consensus mechanism

To solve problems like scalability, latency, and the extra communication associated with delegated proof of stake (DPOS) and Practical Byzantine Fault Tolerant (PBFT), a new consensus algorithm known as HD-LBFT was created. The HD-LBFT protocol uses a dynamically selected subset of representative nodes arranged in a hypergraph structure, as opposed to traditional approaches that demand involvement from each node. From this group, a leader node is chosen to supervise the consensus-building procedure. In large-scale BC applications, HD-LBFT significantly reduces communication complexity, increases performance. Furthermore, by limiting the number of sub-nodes and using dynamic layer rotation, the network is not constrained. To protect network security and integrity, this adaptive rotation technique isolates malicious or defective nodes while preventing single-node dominance and single points of failure. The proposed consensus algorithm is an adaptive version of the BFT [26] protocol. Achieving consensus in a blockchain network is crucial for ensuring that messages are properly shared among all nodes. The proposed approach primarily emphasizes extending the operational lifetime of the network nodes, which enhances the efficiency of the network. In this model, three types are nodes are considered: Leader nodes (Chain head), trust nodes, and faulty nodes.

$$LN = \{L_1, L_2, ..., L_n\},\ TN = \{T_1, T_2, ...T_m\},\quad FN = \{F_1, F_2, ... F_k\} \qquad (1)$$

In the BC network, the leader node plays a vital role in overseeing transactions and ensuring their validity, contributing to a robust and trustworthy system. Both trust nodes and faulty nodes submit transactions and take part in the voting process. Furthermore, the network's client nodes (CN) can choose which node will serve as the leader node. Through the maximum number of votes, the leader node is selected among the CN from the voting process. CN can receive the messages from the candidate nodes. Each node's transactions are monitored by the leader node, which provides a way to find the trusted and faulty nodes. In this scheme, the trust nodes are able to present in the BC while the faulty nodes are removed from the BC. The leader node is chosen based on a rotation basis. Further, the candidate nodes (trust nodes) are responsible for electing the leader node.

A consensus algorithm in BC is a method by which all nodes in the network agree on a common outcome, even when there are timing differences in processing information across the network. Nodes gather transaction histories and share blocks with other nodes. The consensus mechanism ensures that blocks are validated and protects the network from malicious nodes. Even if a node tries to alter the system, it guarantees the integrity and

Received: August 11 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

readability of the BC. It is impossible to alter the recorded history because defective nodes cannot alter the transaction history or modify block ownership. There are five main steps in the BFT consensus process:

1. **Leader node selection:** Using voting thresholds and trust ratings, trust nodes vote to choose a leader on a dynamic basis.
2. **Divide nodes:** Based on the transaction behavior, nodes are divided into two groups: defective nodes and trusted nodes.
3. **Find trust nodes:** Trust values are calculated to ensure eligibility for future consensus rounds.
4. **Find faulty nodes:** The consensus network detects and removes malicious nodes.
5. **Leader replacement:** To maintain network lifespan and avoid performance degradation, the leader node is constantly replaced.

Algorithm 1: Leader node selection

Start:

Initialize:

Threshold voting value of

voting of in the network

while

send a request to all client nodes in the network

retrieve from the client node

Calculate No of votes for the client node

calculate

if then

calculate

candidate node is selected as a leader node

End

The leader node selection procedure of a BC network is described in Algorithm 1. The BFT methods select the primary nodes as the chain head in the first step. There are many CN in a distributed BC network. A subset of the client nodes serves as candidate nodes, and the remaining nodes take part in the voting process. The leader node is then selected by all client nodes to serve as the chain leader. The candidate node can then send the request message to the CN. All CNs in the BC network will vote for any candidate after receiving a request message from a single candidate node. Multiple CNs vote for the candidate node

Received: August 11 2025

International Journal of Applied Mathematics

Volume 38 No. 8s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

simultaneously. Finally, find the candidate node that garnered the most votes throughout the voting process. The winner becomes the leader node, and a CN becomes a follower of the leader node. The leader node in the proposed techniques monitors the transactions of the client nodes of the network.

Algorithm 2: Divide nodes

Initialize: $FN \quad and \quad TN, \; netw$

$TN < -\phi \; , \; FN < -\phi$

$\text{for}\,(node \; , \; \in \; netw)$

$\text{if}\, node \; , \; > valid\ transaction \quad of \quad node \;) \; then$

$TN \leftarrow node,$

Else

$FN \leftarrow node$

The BFT technique was described in Algorithm 2. In this algorithm, CNs in the network are divided into two types, namely fault nodes, also referred to as malicious nodes in a BC system, and trust nodes, which are the blockchain network's equivalent of honest nodes. The leader node in a BC system. The leader node monitors the activities of the CN, including identifying legitimate and invalid transactions. A faulty node is one that consistently sends incorrect data to the network. A CN that sends a legitimate transaction into the network is referred to as a trust node.

Algorithm 3: Find trust nodes

Initialize: Val_{Trust}

$Val_{Trust} \leftarrow 0$

for $(node \in TN)$

$T_{scor} = trust(i, j) - untrust\ (i, j)$

$T_{trustvalue} = \sum \max\left(T_{score\ i,j}, j, 0\right)$

IF $(T_{trustvalue} = 0)$ **then**

Set $Val_{Trust} = 1/netw$

else

$Val_{Trust} = \max(T_{score}, 0) \; / \; T_{rustvalue}$

end

Received: August 11 2025

International Journal of Applied Mathematics

Volume 38 No. 8s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Algorithm 3 described how a trusted node was determined using the total number of valid transactions in the network. The trust node is the third stage in the adaptive BFT algorithm. Nodes are permitted to take part if the client node is a trust node. Describes the voting process and sends the legal transaction to the network. These trusted nodes may eventually act as candidate nodes in the voting process. Because this approach only allows for increased trust nodes, network lifetime, packet delivery rate and performance.

Algorithm 4: Find faulty nodes

Let $FN_{i,j}V$ is the faulty node transaction value

$Val_{Trust} \leftarrow 0$

Find transaction value between nodes $node_j \in faulty\ node$

For $(node_j \in faulty\ node)$

If $\left(node_{i,} \in TN\ node_{i,j} \in TN\right)$

$Val_{Trust\ i,j} = \sum Val_{Trust\ i,j} Co_{i,g}$

Else

Compare $Val_{Trust\ i,j}$ iteratively

The identification of the network failed node from the trusted node was clarified by algorithm 4. The fault node is eliminated from the voting process while the problematic node is identified using this approach. In this case, the faulty nodes cannot participate in the voting process, by using this method helps to reduce the network partition.

Algorithm 5: Leader replacement

Manage the leader node.

$RC = LN\ round\%update$ int $erval$

If $RC = 0$

$LN\_RC = change\ LN()$

If $(Energy < Energy\ of\ Threshold\ \ node\ in\ the\ network)$ then

$re-construct\ \ LN$

Update the Routing table.

Else

Received: August 11 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

$$LN\ rotation = same\ \ LN()$$

According to Algorithm 5, a rotation strategy should be used to continuously change the leader node. This is used to extend the lifetime of networks. A dead node occurs when the same node serves as the leader for a long time. Here, to make the network last longer, switch out the leader node and update the routing table often. Using this technique, the other trust node can also act as a primary node on a rotational basis. For a BC network to function properly and provide reliable judgments, it requires a minimum number of nodes. There is one trusted node in the quorum. To prevent this blockchain network from shutting down, there must be at least one malicious node in the equation.

3.2 Semantic-Aware Gradient-Driven Gossip Protocol

The proposed technique, called Semantic-Aware Gradient-Driven Gossip (SAGD-Gossip) protocol, is used to improve the scalability, reliability and efficiency of information distribution in decentralized networks. Traditional gossip methods broadcast all messages indiscriminately, which leads to additional processing cost, increased latency and duplicate traffic. SAGD-Gossip uses gradient driven and semantic awareness to ensure that only relevant messages are sent in the most efficient ways. The semantic awareness component integrates two complementary techniques, such as semantic filtering and semantic aggregation.

3.2.1 Semantic filtering

The semantic filtering is a method that reduces duplicate and outdated messages during distribution. In contrast to conventional gossip protocols, semantic filtering determines which messages should be disseminated based on the importance to the consensus process that reports all messages randomly. There are procedures to identify communications that aren't necessary for moral reasons, and all incoming messages are thoroughly reviewed for bias. The following are important building guidelines:

1. Duplicate suppression: Messages that have the same parameters (types, origin, height, round, and block ID)
2. Post-Quorum suppression: Subsequent messages of the same type are filtered out once a certain round has a quorum of valid votes.

This method preserves system accuracy and dependability while reducing processing overhead, propagation latency and network congestion.

3.2.2 Semantic awareness

Semantic aggregation reduces the overall size of messages sent by combining multiple semantically comparable messages into a single, condensed message before distribution. The steps in the aggregation process include finding relevant messages, creating a unified message and sharing. The types of aggregation include such as:

1. Reversible aggregation: The Initial message can be reconstructed.

Received: August 11 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

2. Non-reversible aggregation: The consensus protocol processes the aggregated message directly.

Aggregation is used in the BC consensus for messages with the same parameters, such as PREVOTE and PRECOMMIT. A set of <origin, signature> pairs and the desired block are included in the synthesized message. Benefits include reduced bandwidth consumption, low processing overhead and fast propagation while the consensus preserves correctness.

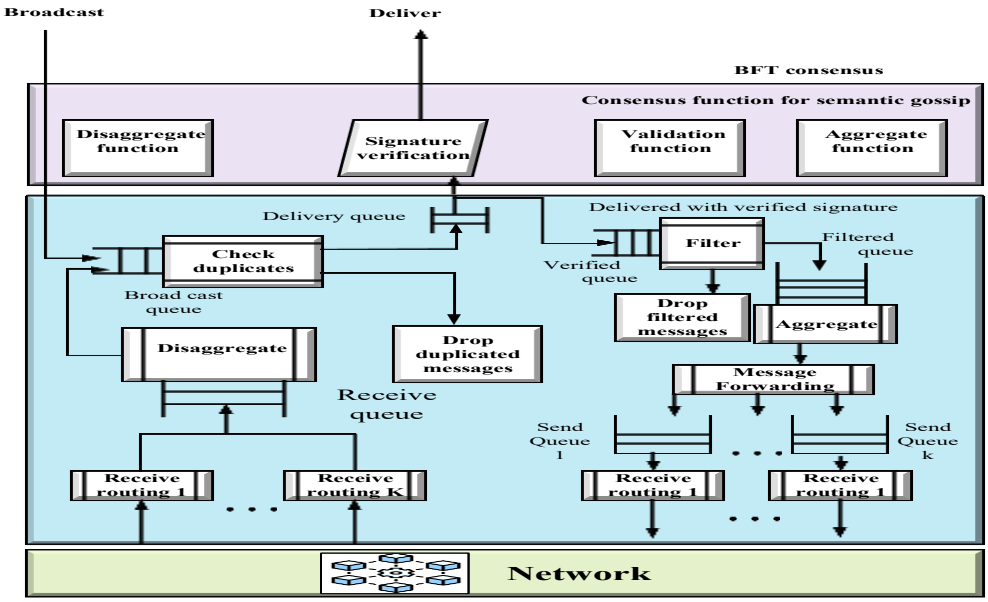

Figure 2: The architecture of semantic gossip

Figure 2 shows the architecture of semantic gossip. The process of semantic filtering is achieved by using a function of consensus function. When a message reaches the gossip layer, the filter module invokes this function to determine whether it should be forwarded or discarded. If the function returns false, the message will be deleted as irrelevant, invalid or duplicate. On the other hand, if it returns true, the message will be sent to the target user. Since the verification process can be carried out simultaneously across multiple communication process, it must be fast and seamless to provide scalability. This method balances the storage required to handle message states, reducing the network traffic required.

Semantic aggregation reduces communication overhead and bandwidth utilization by compressing several semantically linked messages into a single, concise message using two procedures that are implemented in the consensus layer, namely , before distribution. In situations where aggregation is reversible, the gossip layer uses a splitting operation to reconstruct the original message after receiving the aggregated message. To prevent recurrence, this procedure ensures that messages are handled in the correct order and compared with recently received data. By lowering the overall number of messages sent, semantic aggregation increases network efficiency and propagation speed while preserving the precision of the underlying consensus process. The gradient driven routing pulls requests along efficient paths established by an application gradient that takes into account message priority, node responsiveness, and network latency. Gradient-driven propagation increases

Received: August 11 2025

Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

message propagation. Nodes prevent indiscriminate loading and flexibly adjust to changing network conditions by reusing only data frame neighbors with high utilization. This technology improves network speed, reduces duplicate traffic and increases product lead time.

3.2.3 Semantic Gossip

Conventional gossip systems send all communications randomly and treat the content of messages as ambiguous. However, semantic gossip [27] makes sure that only relevant information spreads throughout the network by basing sharing options on the semantics of messages. This approach can be vulnerable in the presence of Byzantine nodes since bad nodes can employ aggregation or semantic filtering to stop propagation. Semantic gossip integrates signature verification into the consensus layer to address the following issues:

Before the gossip layer processes a message, it is authentically verified.

Semantic structuring and aggregation are performed after a recognized content in the semantic gossip layer, which retrieves only verifiable matches.

This design eliminates unnecessary validation in the rumor layer and ensures that sharing decisions rely only on valid messages, which preserves the BFT properties of the underlying consensus protocol.

Result and Discussion

In this section, the performance is evaluated based on the existing and proposed models. The key indicators, such as transaction confirmation latency, throughput (TPS), scalability nodes, consensus success rate, block reception delay, and block propagation delay, are used to assess the BC network performance. The results demonstrate increased speed, dependability, and resource usage, as well as reduced latency and increased throughput. Additionally, the network demonstrates performance and resilience by continuing to operate smoothly even with byzantine nodes.

4.1 Performance evaluation for BC network

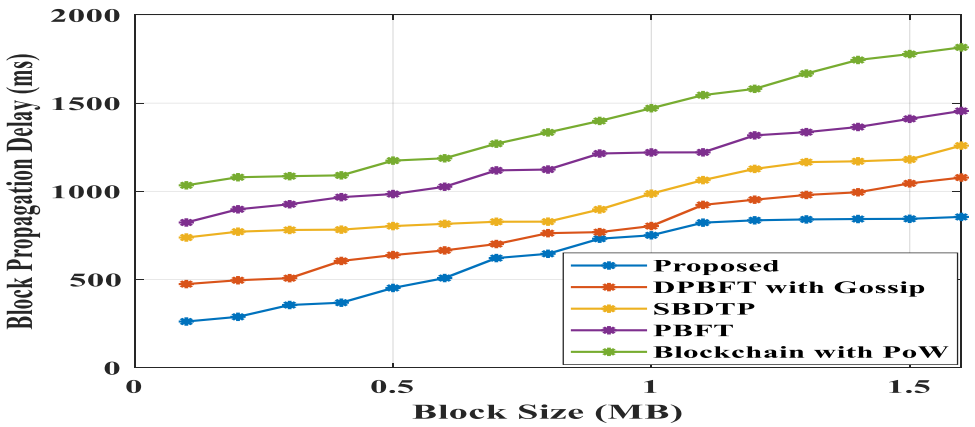

Figure 3: Analysis of Block propagation delay for existing and proposed models

Received: August 11 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Figure 3 illustrates the performance of the proposed model by evaluating the block propagation delay. The existing models, such as DPBFT with Gossip with 473.84 ms, SBDTP with 737.97 ms, PBFT with 823.23 ms and Blockchain with PoW attained 1033.96 ms, while the proposed model achieved a delay of 261.57 ms for a 0.1 MB block size. The proposed model consistently outperformed the existing models, with a range of DPBFT with Gossip with 495.60 ms, SBDTP with 771.07 ms, and PBFT with 897.97 ms and Blockchain with PoW attained 1079.72 ms, while the proposed model achieved a delay of 288.18 ms for a 0.2 MB block size. Similarly, the proposed model consistently found lower values than existing models from 0.2 MB to 1.6 MB block size. The Block propagation delay comparison between the proposed model and existing consensus techniques for varying block sizes is shown in Table 2.

Table 2: Block propagation delay

Block size (MB)	**Proposed**	**Blockchain with PoW**	**DPBFT with Gossip**	**SBDTP**	**PBFT**
0.1	261.5712	1033.965443	473.8364052	737.9724	823.2378
0.2	288.1833	1079.726707	495.6025077	771.0798	897.9783
0.3	355.2207	1085.925264	507.4686682	780.7194	926.6653
0.4	368.3132	1090.390779	605.1267059	782.5839	966.8342
0.5	451.9129	1173.995253	638.2611735	802.7822	984.4634
0.6	508.1187	1187.180803	664.9364831	815.395	1025.818
0.7	621.3993	1269.924678	701.0385727	827.3729	1118.582
0.8	645.5741	1333.991615	762.5957052	827.9167	1123.444
0.9	731.1761	1399.120276	768.5095115	896.9906	1214.268
1	750.6046	1471.086409	802.9743959	986.5264	1220.334

Received: August 11 2025

Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

1.1	822.2227	1545.478719	922.9076723	1063.401	1220.898
1.2	835.5736	1581.005385	952.5098004	1127.045	1317.19
1.3	840.5478	1667.596669	979.3811939	1165.585	1335.491
1.4	842.8735	1744.771941	994.5267751	1170.166	1364.73
1.5	843.9492	1778.331893	1044.970268	1180.72	1410.869
1.6	854.774	1816.271611	1077.899768	1259.083	1455.613

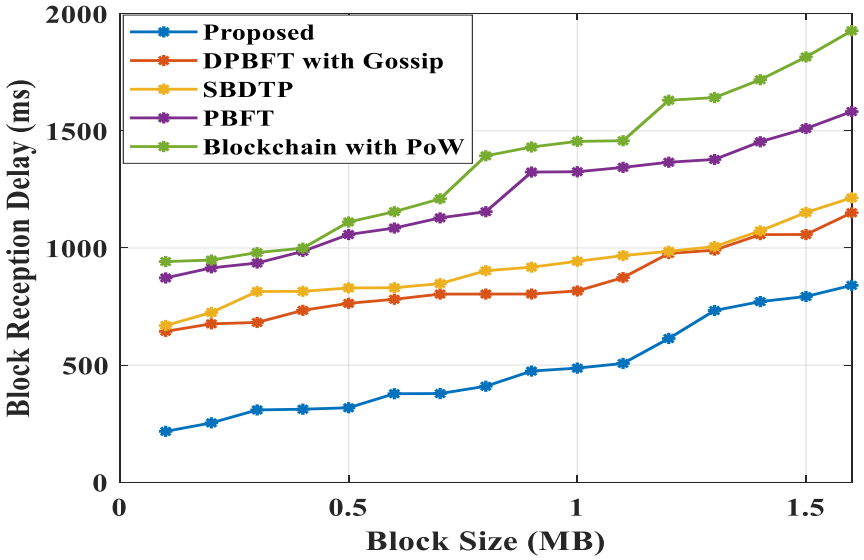

Figure 4: Block reception delay for existing and proposed models

The block reception delay for various block sizes is shown in Figure 4. The proposed model achieved 217.11 ms for 0.1 MB, compared to existing models such as DPBFT with Gossip, with 644.12 ms, SBDTP with 668.92 ms, PBFT with 872.05 ms, and Blockchain with PoW attained 941.98 ms. Similarly, the proposed model consistently reported short delays for block sizes ranging from 0.3 MB to 1.6 MB. In contrast, the proposed model consistently recorded lower values, while existing models continued to show higher ranges. This illustrates the benefits of the proposed architecture in terms of faster batch processing, lower latency and increased network performance. Table 3 shows the block reception delay comparisons.

Received: August 11 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Table 3: Block Reception delay

Block size (MB)	Proposed	DPBFT with Gossip	SBDTP	PBFT	Blockchain with PoW
0.1	217.1126	644.124633	668.922	872.0541	941.9865442
0.2	253.3511	676.1102287	724.6806	915.0923	948.3469815
0.3	308.6321	682.0708047	814.1594	935.7666	980.3171008
0.4	311.7009	733.7742293	814.8525	985.4722	999.2391504
0.5	317.9386	763.7044705	829.3089	1057.407	1110.859494
0.6	377.8485	781.048816	830.1136	1085.002	1154.814855
0.7	378.5713	803.0923349	847.8854	1128.504	1209.754709
0.8	409.7746	803.2475086	902.8898	1154.905	1393.379771
0.9	474.5619	803.481632	918.0331	1323.992	1430.960525
1	487.0924	816.5698684	943.1015	1325.417	1455.033058
1.1	507.1722	873.5921781	967.406	1343.944	1457.673003
1.2	613.6775	976.476429	985.7284	1365.987	1630.53138
1.3	732.9115	990.7664298	1005.861	1377.781	1641.899149
1.4	771.0227	1057.020739	1072.885	1453.416	1718.164984
1.5	792.8955	1057.430879	1151.552	1509.875	1815.243959

Received: August 11 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

1.6	840.4693	1150.337964	1214.248	1582.372	1927.297455

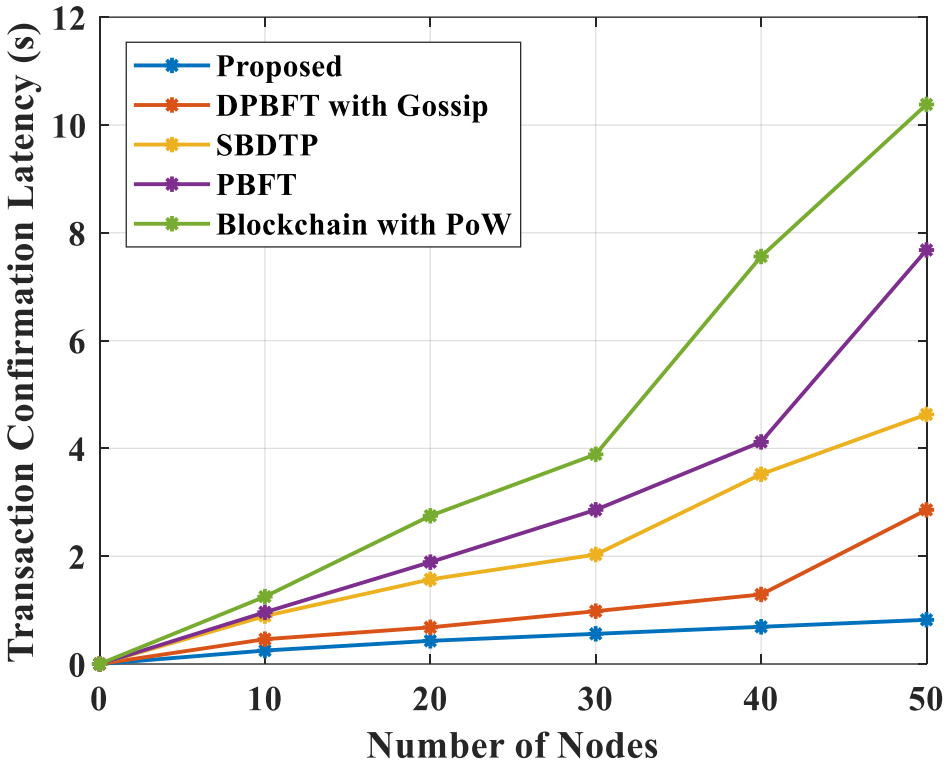

Figure 5: Analysis of Transaction confirmation latency

Figure 5 shows the comparison of the proposed model with existing models of transaction confirmation latency for varying node counts. The proposed model had a lowest latency of 0.25 across 10 nodes, compared to existing models such as DPBFT with Gossip with 0.46 s, SBDTP with 0.89 s, PBFT with 0.96 s and Blockchain with PoW attained 1.25 s. The proposed latency on node 20 attained a lower latency of 0.43 s, but other existing models showed higher latency of DPBFT with Gossip with 0.68 s, SBDTP with 1.57 s, PBFT with 1.89 s, and Blockchain with PoW attained 2.7 s. Similarly, the proposed model consistently maintained reduced latency for 30 to 50 nodes, while the existing models showed a significant increase in latency. The specific transaction details are shown in Table 4.

Table 4: Transaction confirmation latency

Number of Nodes	Transaction Confirmation Latency (s)				
	Proposed	DPBFT with Gossip	SBDTP	PBFT	Blockchain with PoW
0	0	0	0	0	0
10	0.25	0.46	0.89	0.96	1.25

Received: August 11 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

20	0.43	0.68	1.57	1.89	2.75
30	0.56	0.98	2.03	2.86	3.89
40	0.69	1.29	3.52	4.12	7.56
50	0.82	2.86	4.63	7.68	10.38

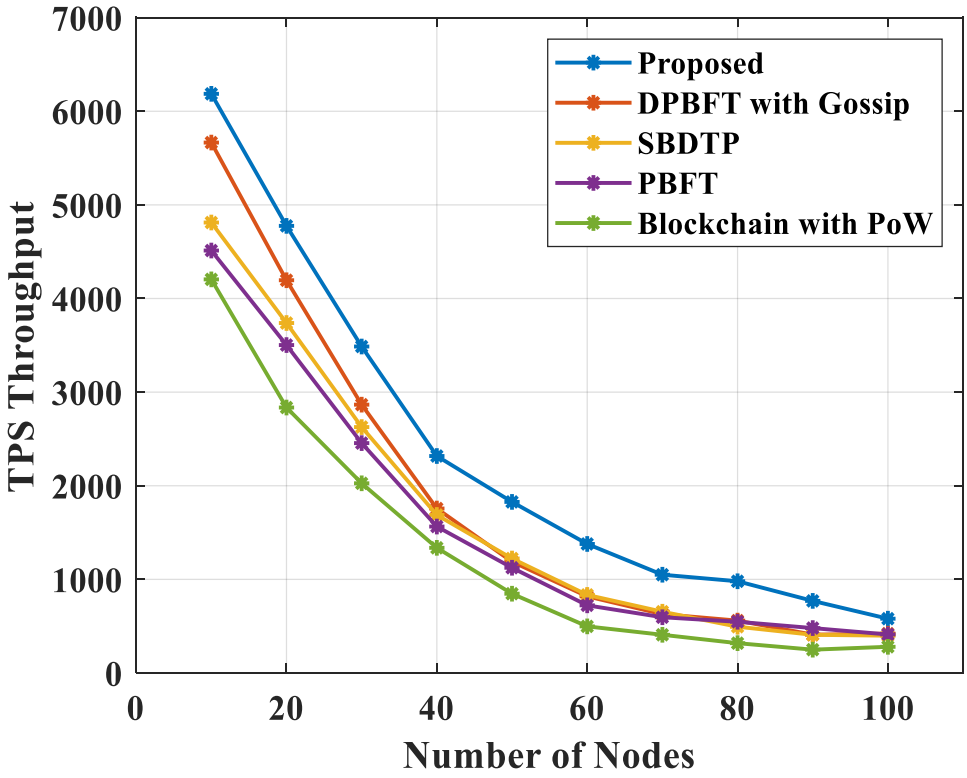

Figure 6: Analysis of Throughput with existing and proposed models

The throughput performance comparison of 10-100 nodes is shown in Figure 6. The existing model performed DPBFT with Gossip with 5665.57 TPS, SBDTP with 4811.55 TPS, PBFT with 4512.39 TPS and Blockchain with PoW attained 4204.31 TPS on 10 nodes, while the proposed model achieved 6186.04 TPS. The existing model saw significant declines, including DPBFT with gossip 420.32 TPS, SBDTP with 398.71 TPS, PBFT with 411.61 TPS and Blockchain with PoW attained 279.85 TPS across 100 nodes. This illustrates the inherent scalability and performance of the proposed framework. The corresponding values are listed in Table 5.

Table 5: TPS Throughput

Number of Nodes	**Transaction Confirmation Latency (s)**				
	Proposed	**DPBFT with Gossip**	**SBDTP**	**PBFT**	**Blockchain with PoW**

Received: August 11 2025

International Journal of Applied Mathematics

Volume 38 No. 8s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

0	0	0	0	0	0
10	0.25	0.46	0.89	0.96	1.25
20	0.43	0.68	1.57	1.89	2.75
30	0.56	0.98	2.03	2.86	3.89
40	0.69	1.29	3.52	4.12	7.56
50	0.82	2.86	4.63	7.68	10.38

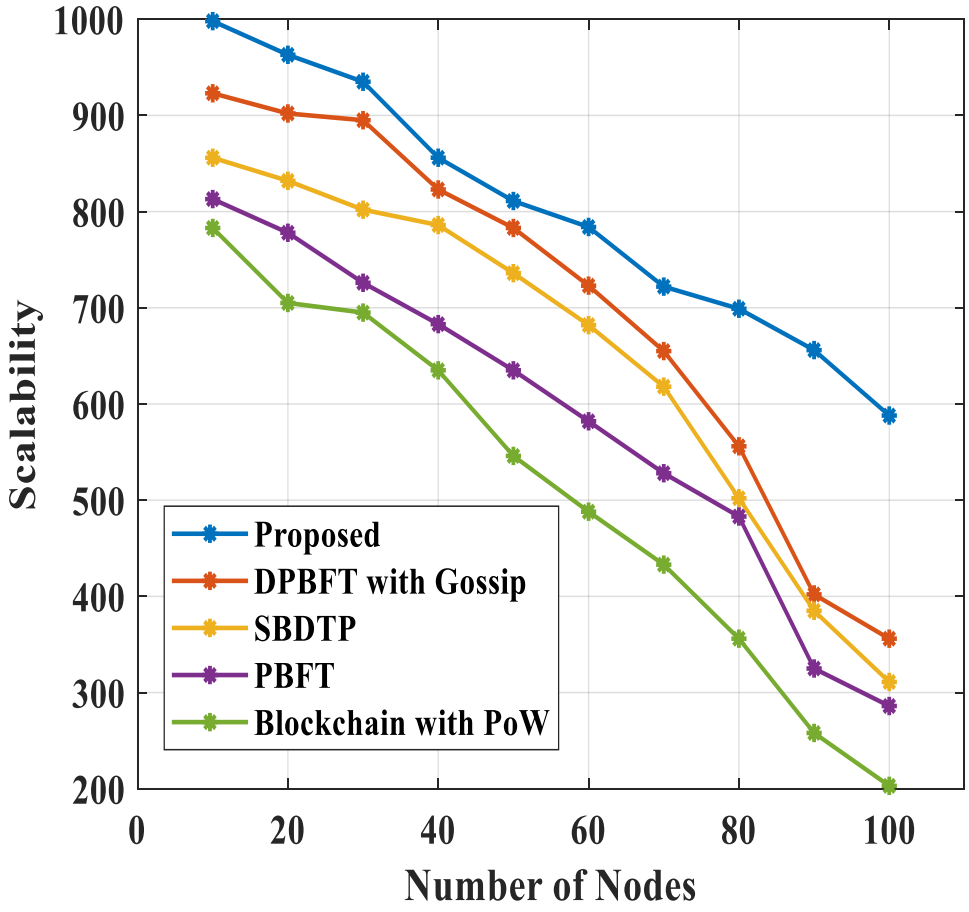

Figure 7: Analysis of scalability nodes

For network sizes ranging from 10 to 100 nodes, Figure 7 compares the scalability of the proposed model with existing models. The existing models, such as DPBFT with Gossip with 923, SBDTP with 856, PBFT with 813 and Blockchain with PoW attained 783, while the proposed model achieves the largest scalability of 998 across 10 nodes. However, the proposed model held a strong score of 588 on 100 nodes, while DPBFT with Gossip with 356, SBDTP with 311, PBFT with 286 and Blockchain with PoW attained 203. This illustrates how robust and scalable the proposed framework is over existing consensus methods. The specific scalability values are shown in Table 6.

Received: August 11 2025

International Journal of Applied Mathematics

Volume 38 No. 8s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Table 6: Scalability

Number of Nodes	Transaction Confirmation Latency (s)				
	Proposed	DPBFT with Gossip	SBDTP	PBFT	Blockchain with PoW
0	0	0	0	0	0
10	0.25	0.46	0.89	0.96	1.25
20	0.43	0.68	1.57	1.89	2.75
30	0.56	0.98	2.03	2.86	3.89
40	0.69	1.29	3.52	4.12	7.56
50	0.82	2.86	4.63	7.68	10.38

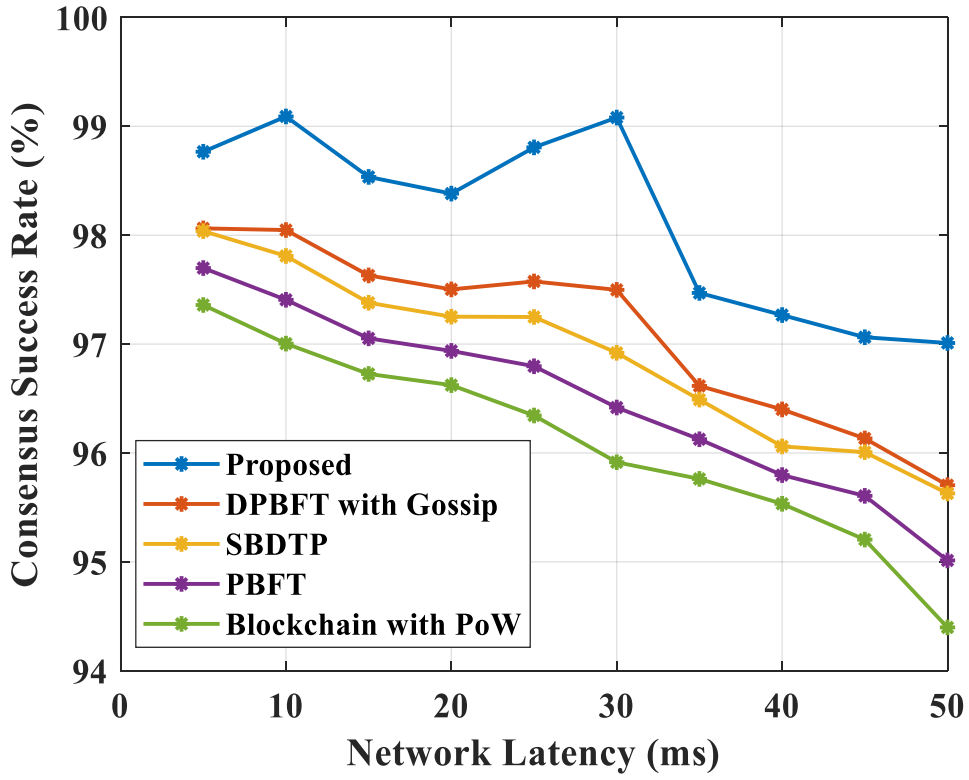

Figure 8: Performance analysis of consensus success rate

The consensus rate of the proposed model was evaluated under various network delays and compared to Blockchain with PoW, SBDPT, PBFT and DPBFT with gossip, as shows in Figure 8. The proposed framework consistently produced the great success rates of 98.77%, 99.09%, 98.54% and 98.38% at latencies of 5 ms, 10 ms, 15 ms and 20 ms, respectively. In comparison to DPBFT with gossip, which obtained success rates of 98.06%, 98.05%, 97.63% and 97.50% at the same latencies. These outcomes show how resilient and dependable the

Received: August 11 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

proposed approach is when network latency increases. Table 7 shows the consensus success rate comparison.

Table 7: Consensus success rate

Network Latency (ms)	Consensus Success Rate (%)				
	Proposed	DPBFT with Gossip	SBDTP	PBFT	Blockchain with PoW
5	98.76653	98.06276	98.03755	97.69827	97.35899
10	99.09056	98.047345	97.8092	97.40667	97.00413
15	98.53519	97.63044	97.3795	97.0526	96.72569
20	98.38196	97.502435	97.25135	96.93713	96.62291
25	98.80653	97.57525	97.24874	96.79636	96.34397
30	99.08065	97.497795	96.9198	96.41737	95.91494
35	97.46979	96.615665	96.48981	96.12568	95.76154
40	97.26639	96.39962	96.06028	95.79657	95.53285
45	97.06278	96.133405	96.0075	95.60577	95.20403
50	97.01013	95.703745	95.62818	95.01277	94.39736

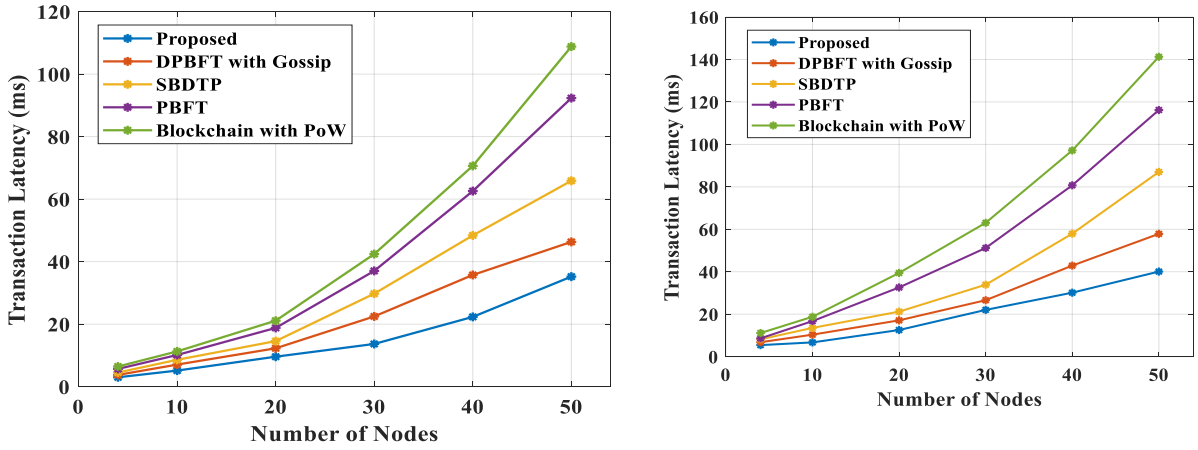

Figure 9: Performance analysis of (a) transaction latency without byzantine nodes, (b) transaction latency with byzantine nodes

Figure 9(a) and (b) show the performance analysis of transaction latency without byzantine nodes and transaction latency with byzantine nodes. Figure 9 (a) compares the transaction latency of the proposed consensus framework with existing models. The proposed model demonstrated greater scalability and efficiency were demonstrated with its constant reduced latency, which varied from 2.99 ms at 4 nodes to 35.20 ms at 50 nodes. In contrast, DPBFT with gossip ranged from 3.76 ms to 46.32 ms. Figure 9(b) compares the transaction latency of the proposed consensus architecture with byzantine nodes to that of existing models as

Received: August 11 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

network sizes increase to 4, 10, 20, 30, 40 and 50 nodes. The proposed model consistently lowered latency from 5.42 ms at 4 nodes to 40.07 ms at 50 nodes. In contrast, the DPBFT with Gossip ranged between 6.79 ms and 57.84 ms, demonstrating the proposed architecture's effectiveness and resilience in hostile situations. Transaction latency without byzantine nodes, transaction latency with byzantine nodes, is shown in Table 8.

Table 8: Transaction latency without byzantine nodes, transaction latency with byzantine nodes

Number of Nodes	**Transaction Latency (ms) without byzantine nodes**	**Transaction Latency (ms) with byzantine nodes**
	Proposed	**DPBFT with Gossip**
4	2.99124	3.75801
10	5.13985	7.05514
20	9.58549	12.27414
30	13.66093	22.46728
40	22.31887	35.7308
50	35.20396	46.31557

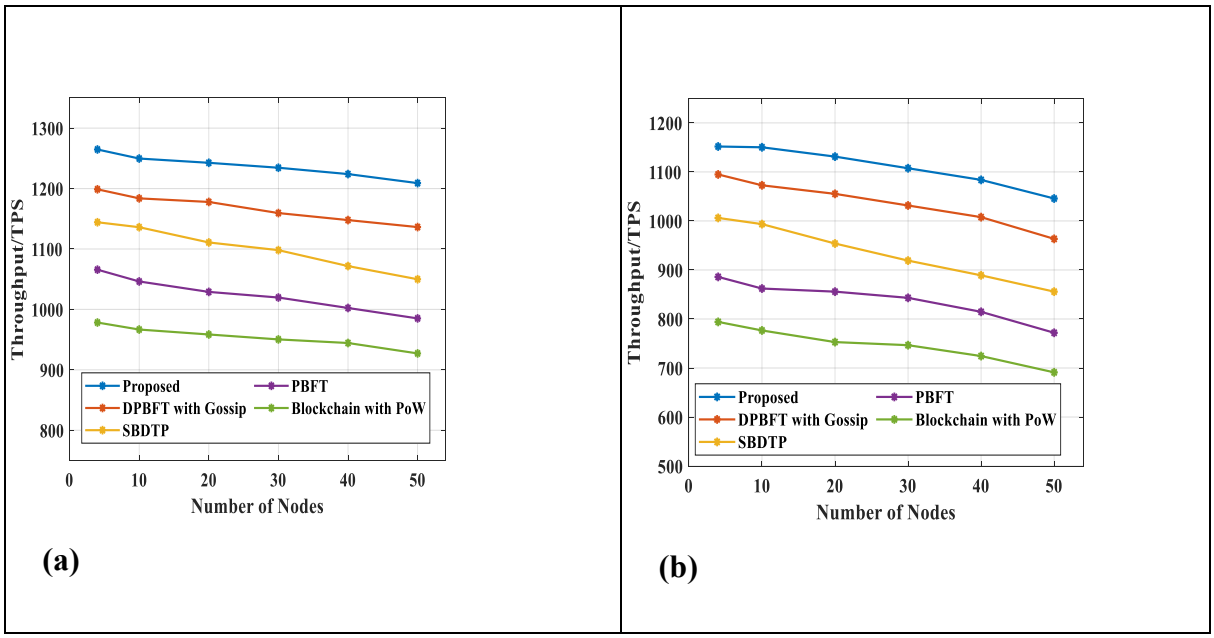

Figure 10: Comparison of (a) throughput without byzantine nodes, (b) throughput with byzantine nodes

The comparison of throughput without byzantine nodes and throughput with byzantine nodes is shown in Figure 10 (a-b). Under growing network sizes without byzantine nodes, Figure 10

Received: August 11 2025

International Journal of Applied Mathematics
Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

(a) shows the performance of the proposed consensus framework in comparison with Blockchain with PoW, DPBFT with gossip, SBDTP, and PBFT. Starting at 1214.66 TPS for 4 nodes, gradually decreasing to 1158.99 TPS for 50 nodes, the proposed approach consistently produced the highest performance. Comparatively, SBDTP ranges from 1094.20 TPS to 999.89 TPS, PBFT from 1015.79 TPS to 877.17 TPS and DPBFT with gossip varies from 1148.74 TPS to 1086.25 TPS. These results demonstrate the exceptional scalability and performance of the proposed model. As the network sizes increase to 4, 10, 20, 30, 40 nodes, Figure 10(b) compares the performance of the proposed consensus architecture with Byzantine nodes to SBDTP, PBFT, Blockchain with PoW and DPBFT with gossip. Starting at 1151.85 TPS for 4 nodes to 1045.78 TPS for 50 nodes, the proposed approach consistently produced the highest performance. On the other hand, DPBFT with Gossip varies between 1094.85 TPS and 963.46 TPS at nodes 4 to 50. These outcomes show how effective and resilient the proposed framework is in hostile environments. Throughput without byzantine nodes, throughput with byzantine nodes is given in Table 9.

Table 9: Throughput without byzantine nodes, throughput with byzantine nodes

Number of Nodes	**Throughput without byzantine nodes (TPS)**	**Throughput with byzantine nodes (TPS)**
	Proposed	**DPBFT with Gossip**
4	1214.655	1148.74006
10	1199.658	1133.75126
20	1192.626	1127.84049
30	1184.447	1109.43835
40	1173.98	1097.83295
50	1158.987	1086.25109

Discussion

Several consensus and gossip-based protocols, such as PoW, PBFT, SBDTP, and DPBFT plus gossip, have been employed to enhance the performance of blockchain networks. However, these models have the some limitations, like unnecessary message propagation, high transmission costs, high latency and poor scalability. PoW used a lot of processing power, but because of leader reliance, PBFT and DPBFT had trouble with network congestion and bottlenecks. To overcome these issues, this study combines the SAGD-Gossip protocol with the HD-LBFT consensus. SAGD-Gossip intelligently filters and combines messages, which reduces redundancy, while the HD-LBFT method uses Hypergraph structures to increase the efficiency of leader selection and verification. The experimental evaluation shows that the proposed architecture improves BC performance. Specifically, it achieves 0 transaction confirmation latency with 0 nodes, 261.5712 block propagation latency with 0.1 MB block

Received: August 11 2025

Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

size, 217.1126 block reception latency with 0.1 MB block size, and 6186.048 transactions per second (TPS) performance with 10 nodes. Additionally, it supports the processing and communication expenses, increasing the scalability and security of the blockchain network.

Conclusion

This study examines key performance metrics such as transaction confirmation latency, communication cost, block propagation delay, and throughput with the aim of enhancing the performance, scalability, and security of BC networks. The suggested architecture enhances BC performance in terms of transaction confirmation latency, block propagation delay, block reception latency, and TPS performance, according to experimental evaluation. The model obtained a delay of 6186.048 with 10 nodes in total. There were 261.5712 nodes in use, and the block size was 0.1 MB. Despite these advancements, BC systems continue to encounter difficulties while functioning in dynamic and expansive settings, including significant communication overhead, verification latency and restricted scalability. Reliable and secure operation, especially in applications that require fault tolerance and real-time processing, depends on solving these problems. To further reduce latency and increase performance, future research could focus on combining adaptive optimization algorithms, intelligent routing systems and sophisticated cryptographic approaches. To enable decentralized applications in various sectors, ensuring security and performance at scale, it is essential to explore lightweight and energy-efficient solutions.

References

[1] Gong, Yi, Boyuan Yu, Lei Yang, Fanke Meng, Lei Liu, Xinjue Hu, and Zhan Xu. "Toward next-generation networks: A blockchain-based approach for core network architecture and roaming identity verification." Digital Communications and Networks 11, no. 2 (2025): 326-336.

[2] Lee, Hye Jin, Duc Anh Luong, Jong Hwan Park, and Hyoseung Kim. "Blockchain-Based Anonymous Reputation System for Performance Appraisal." IEEE Access (2025).

[3] Sachithanandam, Vidhya, D. Jessintha, Hariharan Subramani, and V. Saipriya. "Blockchain integrated multi-objective optimization for energy efficient and secure routing in dynamic wireless sensor networks." Sustainable Computing: Informatics and Systems 46 (2025): 101101.

[4] Guo, Shaolong, Yuntao Wang, Ning Zhang, Zhou Su, Tom H. Luan, Zhiyi Tian, and Xuemin Shen. "A survey on semantic communication networks: Architecture, security, and privacy." IEEE Communications Surveys & Tutorials (2024).

[5] Wei, Yuecen, Xingcheng Fu, Dongqi Yan, Qingyun Sun, Hao Peng, Jia Wu, Jinyan Wang, and Xianxian Li. "Heterogeneous graph neural network with semantic-aware differential privacy guarantees." Knowledge and Information Systems 65, no. 10 (2023): 4085-4110.

[6] Kim, Sungbeen, and Dohoon Kim. "Data-tracking in blockchain utilizing hash chain: a study of structured and adaptive process." Symmetry 16, no. 1 (2024): 62.

Received: August 11 2025

Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[7] Jabar, Mohanad Sameer. "Blockchain-enabled Secure Data Communication Protocols for 5G Networks." Engineering, Technology & Applied Science Research 15, no. 1 (2025): 20151-20161.

[8] Subramanian, N. Sethu, Prabhakar Krishnan, Kurunandan Jain, KB Aneesh Kumar, Tulika Pandey, and Rajkumar Buyya. "Blockchain and RL-Based Secured Task Offloading Framework for Software-Defined 5G Edge Networks." IEEE Access (2025).

[9] Sasikumar, A., Logesh Ravi, Malathi Devarajan, A. Selvalakshmi, Abdulaziz Turki Almaktoom, Abdulaziz S. Almazyad, Guojiang Xiong, and Ali Wagdy Mohamed. "Blockchain-assisted hierarchical attribute-based encryption scheme for secure information sharing in industrial internet of things." IEEE Access 12 (2024): 12586-12601.

[10] Zhou, Yufei, Rui Han, and Yang Li. "A Blockchain Network Communication Architecture Based on Information-Centric Networking." Applied Sciences 15, no. 6 (2025): 3340.

[11] Wira, Samsuddin Samsuddin, Chee Keong Tan, Wai Peng Wong, and Ian KT Tan. "Cloud-native simulation framework for gossip protocol: Modeling and analyzing network dynamics." PLoS One 20, no. 6 (2025): e0325817.

[12] Weerasinghe, Nisita, Tharaka Hewa, Madhusanka Liyanage, Salil S. Kanhere, and Mika Ylianttila. "A novel blockchain-as-a-service (BaaS) platform for local 5G operators." IEEE Open Journal of the Communications Society 2 (2021): 575-601.

[13] Bala, R., and R. Manoharan. "Blockchain based secure and effective authentication mechanism for 5G networks." In 2022 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), pp. 1-6. IEEE, 2022.

[14] Jiang, Jing, Yudong Wang, and Peizhe Xin. "Blockchain technology enabled communication network for 5G MEC architecture of smart grids." In 2022 IEEE 8th International Conference on Computer and Communications (ICCC), pp. 253-257. IEEE, 2022.

[15] Femminella, Mauro, and Gianluca Reali. "Gossip-based monitoring protocol for 6G networks." IEEE Transactions on Network and Service Management 20, no. 4 (2023): 4126-4140.

[16] Poongodi, M., Mohit Malviya, Mounir Hamdi, V. Vijayakumar, Mazin Abed Mohammed, Hafiz Tayyab Rauf, and Kawther A. Al-Dhlan. "5G based Blockchain network for authentic and ethical keyword search engine." IET Communication. 16, no. 5 (2022): 442-448.

[17] Rahman, Anichur, Md Saikat Islam Khan, Antonio Montieri, Md Jahidul Islam, Md Razaul Karim, Mahedi Hasan, Dipanjali Kundu, Mostofa Kamal Nasir, and Antonio Pescapè. "BlockSD-5GNet: Enhancing security of 5G network through

Received: August 11 2025

Volume 38 No. 8s, 2025
ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

blockchain-SDN with ML-based bandwidth prediction." Transactions on Emerging Telecommunications Technologies 35, no. 4 (2024): e4965.

[18] Balani, Nisha, Pallavi Chavan, and Mangesh Ghonghe. "Design of high-speed blockchain-based sidechaining peer to peer communication protocol over 5G networks." Multimedia Tools and Applications 81, no. 25 (2022): 36699-36713.

[19] Mafakheri, Babak, Andreas Heider-Aviet, Roberto Riggio, and Leonardo Goratti. "Smart contracts in the 5G roaming architecture: the fusion of blockchain with 5G networks." IEEE Communications Magazine 59, no. 3 (2021): 77-83.

[20] Chaudhary, Sachi, Shail Shah, Riya Kakkar, Rajesh Gupta, Abdulatif Alabdulatif, Sudeep Tanwar, Gulshan Sharma, and Pitshou N. Bokoro. "Blockchain-based secure voting mechanism underlying 5G network: A smart contract approach." IEEE Access 11 (2023): 76537-76550.

[21] Haddad, Zaher, Mohamed Baza, Mohamed MEA Mahmoud, Waleed Alasmary, and Fawaz Alsolami. "Secure and efficient AKA scheme and uniform handover protocol for 5G network using blockchain." IEEE Open Journal of the Communications Society 2 (2021): 2616-2627.

[22] Balakumar, D., and S. Nandakumar. "Blockchain-enabled cooperative spectrum sensing in 5G and B5G cognitive radio via massive multiple-input multiple-output nonorthogonal multiple access." Results in Engineering 24 (2024): 102840.

[23] Fei, Shufan, Zheng Yan, Dongliang Wang, Haomeng Xie, Haiguang Wang, and Tieyan Li. "B5G-NFM: Blockchain-Based 5G Network Function Management With Enhanced Security and Privacy." IEEE Transactions on Networking (2025).

[24] Zhan, Yu, Baocang Wang, Rongxing Lu, and Yong Yu. "DRBFT: Delegated randomization Byzantine fault tolerance consensus protocol for blockchains." Information Sciences 559 (2021): 8-21.

[25] Li, Yuxi, Liang Qiao, and Zhihan Lv. "An optimized byzantine fault tolerance algorithm for consortium blockchain." Peer-to-Peer Networking and Applications 14, no. 5 (2021): 2826-2839.

[26] Zhu, Dongxu, and Yepeng Guan. "Mbft: a modular byzantine fault tolerance protocol for high adaptability." Expert Systems with Applications 257 (2024): 125102.

[27] Kaswan, Priyanka, Purbesh Mitra, Arunabh Srivastava, and Sennur Ulukus. "Age of Information in Gossip Networks: A Friendly Introduction and Literature Survey Invited Paper." IEEE Transactions on Communications (2025).

Received: August 11 2025