International Journal of Sciences

Research Article Volume 13 – November 2024 (11)

Enhancing Scalability and Load Balancing through Sharding in Consortium Blockchain-Based Agri-Food Supply Chain System

Xingjian Tian[1]✎, Guangke Qi[1]

[1]Wenzhou Polytechnic, Wenzhou, China

Abstract: Agri-food supply chain is undergoing a transformation towards increasing intelligence and automation with the integration of blockchain technology, particularly consortium blockchains, which are more suitable for realistic applications by offering member management, privacy protection, data auditability and traceability. Despite these advantages, scalability and system performance remain as the bottlenecks. To address this, sharding technology has been adopted but typical sharding protocols such as Relay and Broker are mostly designed for public blockchains and do not harness the potential of consortium blockchains. For that, we designed an agri-food supply chain system model and proposed a new sharding partition algorithm: Weighted and Constrained Label Propagation Algorithm (WCLPA), which brings in the factor of consortium's organization-based weighting accordingly and integrates with BrokerChain, a cutting-edge sharding protocol. Then we tested using a transaction driven simulator, and the evaluation results indicate that our scheme excels in a spectrum of metrics including TPS, confirmation latency, load balancing of transactions and inter-shard transaction ratio. This research signifies a future promising stride towards optimizing consortium blockchain performance in the agri-food supply chain domain through sharding.

Keywords: Agri-Food Supply Chain, Consortium Blockchain, Sharding, Community-Aware Partition

INTRODUCTION

In the domain of agri-food supply chains, the industry has witnessed significant evolution, transitioning from traditional models to more sophisticated systems. Despite advancements, challenges such as transparency, traceability, and the secure management of sensitive data persist**Error! Reference source not found.**. These pain points underscore the need for a robust solution capable of addressing the complex requirements of modern supply chain management.

The advent of blockchain technology offers a promising avenue for addressing these challenges by providing enhancing trust, security, and efficiency within supply chains and ensuring every transaction traceable and verifiable, thereby mitigating risks associated with fraud and improving overall transparency[1]. A typical agri-food blockchain model is as shown in Fig. 1. However, public blockchains lack the regulatory oversight and auditing capabilities necessary in critical fields[2]. This is where consortium blockchains have risen as a viable solution for practical applications by integrating the inherent advantages of blockchain technology with specialized features. These include access control, enhanced privacy protection, member management and data auditability. Such features render consortium blockchains exceptionally suitable for critical sectors, including the agri-food supply chain, which is vital to the nation's economy, security and the well-being of its citizens.

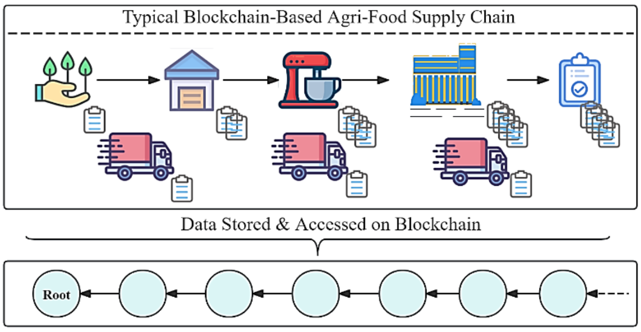

Fig. 1. Blockchain-Based Agri-Food Supply Chain

Despite all the advantages, performance and transaction confirmation latency issues inherent in consortium blockchains present a significant barrier to their widespread adoption. The traditional consensus mechanisms, while secure, often struggle with scalability, leading to bottlenecks in transaction processing and increased confirmation times[3]. To address these issues, sharding technology has been proposed as a future promising solution. Sharding, by dividing the blockchain network into smaller, more manageable pieces, can significantly improve transaction throughput, concurrency performance and reduce transaction confirmation latency.

Existing sharding solutions, however, are predominantly designed for public blockchains and do not fully exploit the potential of consortium blockchains**Error! Reference source not found.**. This realization has prompted us with the design of the Weighted and Constrained Label Propagation Algorithm (WCLPA), a novel shard partition algorithm specifically brings in the degree of physical proximity and network proximity as a weighting factor, thereby enhancing

DOI: 10.18483/ijSci.2808; Online ISSN: 2305-3925; Print ISSN: 2410-4477

✎ Xingjian Tian (Correspondence)
☎ +

transaction balancing, reducing hot-shard issue and improving the overall performance within the agri-food supply blockchain system. The WCLPA was implemented and tested on the BlockEmulator platform, a transaction driven simulator**Error! Reference source not found.**. Through evaluations, we demonstrate that our system not only achieves higher throughput and lower latency but also effectively reduces inter-shard transactions ratio, ultimately aiming to pave the way for more efficient and scalable consortium blockchain-based agri-food supply chain system.

EPRELIMINARIES AND RELATED WORKS

A. Agri-Food Supply Chain and Consortium Blockchain

Traditional agri-food supply chain systems have typically been centralized, leading to significant information asymmetries among various stakeholders. This has resulted in numerous issues such as fraud, tampering, and intermediary attacks, including Sybil and witch attacks. With increasing attention on food safety, traceability of food products has become crucial. Consequently, literature has introduced blockchain technology as a solution to these challenges. An early traceability scheme, HACCP**Error! Reference source not found.** was proposed, integrating blockchain with IoT technologies. However, this scheme was limited by scalability and lacked transparent data flow. Subsequently, hybrid schemes utilizing both on-chain and off-chain databases were proposed[7],**Error! Reference source not found.**, where on-chain stored hashes of data, and off-chain stored the raw data, such as files and addresses of smart contracts. These combined solutions often fall short in security when faced with more sophisticated attacks. To better address security issues, numerous blockchain-based schemes have emerged in recent years**Error! Reference source not found.**,**Error! Reference source not found.**,[11]. However, the decentralization of blockchain technology often conflicts with the management and audit requirements of government institutions, especially in critical areas such as agri-food supply chains, which involve national welfare. As a result, there are relatively few practical applications that have been successfully implemented. To balance the comprehensive needs of security, management, and performance, consortium blockchains have come into the purview of many researchers.

Consortium blockchains are typically composed of participants from a group of consortium organizations. This structure endows consortium blockchains with distinct advantages, such as enhanced control over member and access management, sophisticated data permissions, and comprehensive network monitoring capabilities. The typical roles and operational protocols that characterize consortium blockchains are illustrated in Fig. 2. These features render consortium blockchains particularly well suited for use in government and enterprise contexts, where stringent auditing and management are required. For instance, reference**Error! Reference source not found.** provides a blockchain-based anonymous transportation network system**Error! Reference source not found.** introduces the application of the Bitcoin network to achieve RFID anticloning for security, and designs a supply chain system based on HyperLedger Fabric **Error! Reference source not found.**. However, system performance remains the main bottleneck of this scheme. Overall, the introduction of consortium blockchains offers a more realistic solution for agri-food supply chains, but improving performance, throughput, and reducing latency have become the current primary challenges.

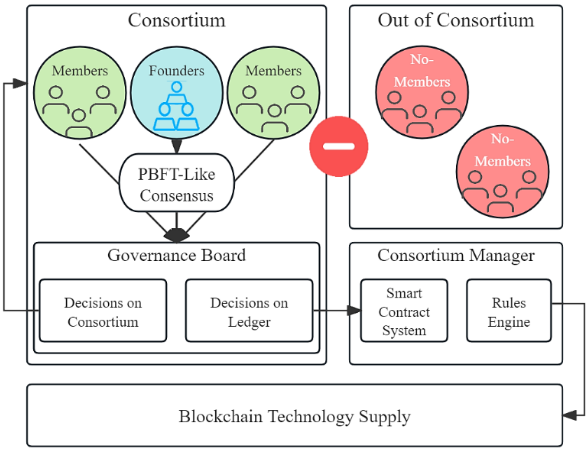

Fig. 2. Typical Consortium Blockchain Architecture

B. Sharding Technology

Sharding technology is a traditional technique from the field of databases, aiming at partitioning a network into several parallel sub-networks to enhance throughput and scalability. In sharding blockchain systems, each shard is only responsible for maintaining the account state for its subset of transactions. Consequently, throughput and concurrency of the entire blockchain system are enhanced**Error! Reference source not found.**.

In blockchain systems that utilize UTXO transaction model, RapidChain**Error! Reference source not found.** and Elastico**Error! Reference source not found.** are representative solutions. RapidChain proposes a mechanism for inter-shard transactions, which transfer involved UTXOs to same shard, thereby transforming inter-shard transactions into intra-shard transactions and ensuring the determinacy of transaction order.

In blockchain systems that adopt account/balance transaction model, the structure typically composes of a final committee, which is also referred to as main shard and several worker shards. Rather than depending on a singular consensus protocol, these systems are inclined to assimilate an ensemble of mechanisms, such as Monoxide**Error! Reference source not found.**, OmniLedger[19], and BrokerChain**Error! Reference source not found.**. Committee members are periodically elected using more secure mechanisms to prevent Sybil attacks and bribery attacks. Nonetheless, the lion's share of the system's performance is attributed to the collective contributions of the worker shards, which, through their coordinated efforts, underpin the blockchain's capacity to meet transactional demands.

However, the handling of inter-shard transactions is a major technique issue due to the existence of hot-shards, which refer to congested shard where transactions cannot be processed in time and usually experience huge confirmation latency, ultimately threatens the eventual atomicity**Error!**

Reference source not found.. These shards usually are caused by active accounts, which launch a large number of transactions frequently in their associated shards. Consequently, transactions are distributed in an imbalanced way. How to reduce count of hot-shards and reach both scalability and load balance when assigning transactions has been the main challenge of sharding blockchains now.

C. Community-Aware Partition

To address the issue of hot-shards, graph theoretic community detection algorithms have naturally garnered the attention of researchers in this field, the idea is shown in Fig. 4. Among these algorithms, LPA is a fundamental technique that operates under the premise of iteratively propagating labels among nodes until a stable community structure is achieved. Nodes initially assign themselves a unique label and subsequently refine these labels by adopting the most common label among their neighbors, leading to the natural emergence of communities.

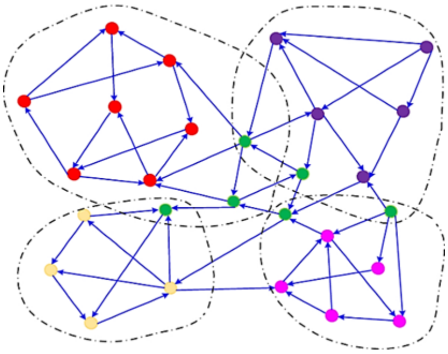

Fig. 4. Community-Aware Partition

There are many algorithms inspired by LPA. For instance, the BrokerChain introduces an iterative threshold to create the Constrained LPA(CLPA)**Error! Reference source not found.**, enables the nodes to be partitioned into the most suitable shards based on transaction frequency. However, BrokerChain is primarily geared towards public blockchain environments and does not fully leverage the advantages inherent in consortium blockchain frameworks. The Weighted LPA(WLPA)[24] introduces weights to the edges of the network, allowing for a more nuanced understanding of relationships between nodes. This weighting scheme accounts for the varying degrees of influence that connections may have, thereby enhancing the accuracy of community detection in weighted networks. The Hierarchical LPA(HLPA) extends the concept further by enabling the detection of communities at multiple levels of granularity**Error! Reference source not found.**. This is particularly useful in networks where a single, flat community structure may not adequately capture the intricate interconnections.

Given the consortium blockchain's characteristics of permissioned member admission and known identities, we have incorporated the role identity of members as a weighting factor in our design of an improved Weighted and Constrained LPA(WCLPA). This approach fully leverages the architectural strengths of consortium blockchains. Detailed algorithmic design and system model specifics will be thoroughly presented in next section.

SYSTEM MODEL

Our proposed agri-food supply chain system model encompasses a hierarchical structure consisting of an application layer and a blockchain layer and ensures full traceability of products from the production phase through to consumption, featuring an intricately designed member identity role system that includes a variety of organizational participants such as producers, collectors, processors, transporters, sellers, and consumers. Furthermore, we elucidate the pivotal smart contracts that are integral to the operation of this system, significantly enhancing its reliability and level of automation.

The first application layer, tailored specifically for the agri-food supply chain, comprises components such as organizational design, member management, transaction model design, and smart contract design. The second layer is the blockchain layer, which is tasked with the implementation of the blockchain network, specific transaction processing, and data storage, encompassing elements such as blockchain network design, the application of sharding technology, and data storage solutions. An overview of the proposed system is depicted in Fig. 5. The subsequent sections will elaborate in detail on the workings of this system.

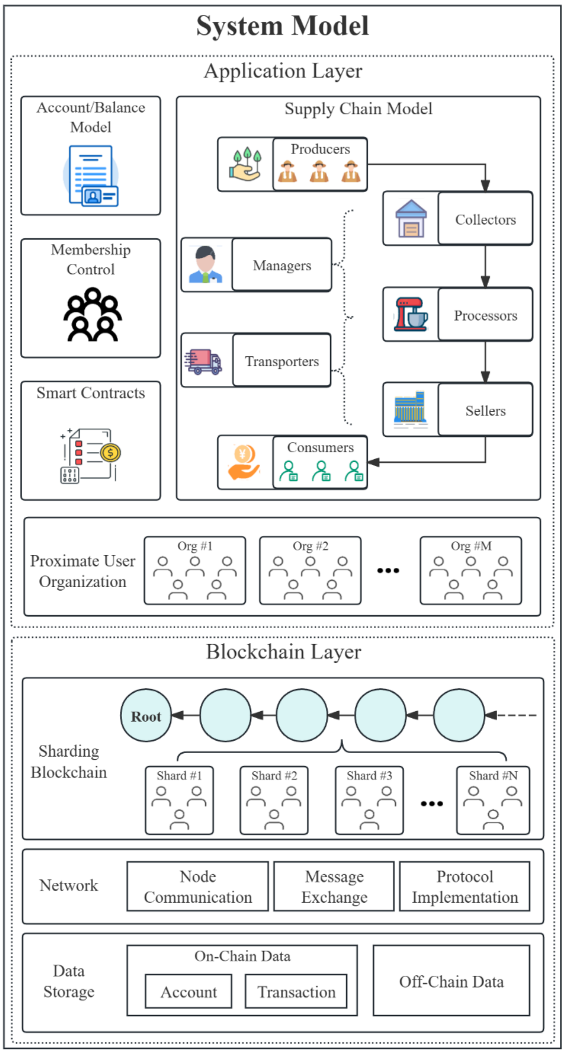

Fig. 5. Proposed System Model of Agri-Food Supply Chain

D. Application Layer

To commence an in-depth exploration of the application layer in our designed system, we begin by highlighting its critical role in orchestrating the interactions and operations within the consortium blockchain framework. This layer serves as the interface above the blockchain network, encapsulating a suite of functionalities that are essential for the seamless execution of supply chain processes.

1) Organization Design: The organizational design within our consortium blockchain system is pivotal, shifting the focus to physical and network proximity of members, advocating for a realistic structure where transactions within an organization are prioritized based on their geographical and operational closeness, thus minimizing latency and improving system performance. In this system, an organization is ideally demarcated by the geographical boundaries of a prefecture-level city, encapsulating all relevant participants within its scope. This approach ensures that transactions occurring within the same organization are assigned higher weights, reflecting the immediacy and frequency of interactions among members.

Nodes within our system can take on any identity, with these identities being directly linked to smart contracts and access permissions. This flexibility allows for a more organic representation of roles and responsibilities, aligning with the diverse and evolving nature of real-world supply chain dynamics. By embracing this organizational design, our system not only enhances the efficiency of intra-organizational transactions but also ensures that the sharding mechanism remains adaptable and responsive to the practical needs of the supply chain, providing a robust foundation for a scalable and effective consortium blockchain architecture.

2) Membership Management: The management of members with different identities, as the inaugural component of this layer, sets the foundation for the security, efficiency, and governance of the entire system. The organizations are described as follows:

- Producers: They are commonly known as farmers and they mark the first in the supply chain and is also the initiator of transactions through smart contracts. Producers cultivate a vast array of crop raw materials, undertaking the critical task of monitoring and documenting the growth details of these crops.
- Collectors: They mainly collect raw materials from producers and then proceed to trim any excess material and distribute and sell the refined products to food processors within their supply network.
- Processors: They are commonly recognized as established food enterprises, and they obtain raw materials from collectors or directly from producers to manufacture food products. They are tasked with documenting the food processing procedures.
- Sellers: They encompass both distributors and retailers, form the next link in the chain. They record the sales data of the finished food products, which ultimately reach the consumers.
- Consumers: They are the end-users who purchase and consume the products from retailers, and they have the ability to access the information of the food product. Once transaction finalized, they can make recorded comments and the transaction data is also recorded on the blockchain, facilitating traceability.
- Transporters: They are responsible for transporting products and are charged with recording transportation data, such as average and peak temperatures, humidity levels, and other relevant metrics.

3) Transaction Model: Within the framework of a consortium blockchain system that incorporates sharding technology, a comprehensive ledger is tasked with recording two distinct types of information: transactions that occur exclusively within a single shard, termed intra-transactions, and those that bridge multiple shards, known as inter-transactions. Capitalizing on the inherent access control and permission management features characteristic of consortium blockchains, our system architecture embraces a streamlined account/balance model, thereby facilitating enhanced efficiency and security in transaction processing.

The transaction process commences with producers, who initiate transactions through smart contracts, laying down the first layer of data that includes material details and quality metrics. This data seamlessly transitions as raw materials are acquired by other members, who update the blockchain with final snapshots and any preliminary processing information. Food processors then document the transformation journey of raw materials into consumable products, capturing critical details such as processing steps and ingredient compositions. Sellers, including distributors and retailers, further augment the data trail with sales transactions, consumer feedback, and distribution metrics. Consumers interact with the blockchain to access full traceability information, making informed purchasing decisions and contributing to the transactional data upon purchase completion.

4) Smart Contracts: Smart contracts are essential to the seamless operation of our system. These contracts are tailored to cater to the distinct needs and functions of each participant within the supply chain, ensuring that the transactions are not only secure but also transparent and efficient. The major smart contracts we designed for each type of identities are listed in Table. 1.

TABLE 1
MAJOR SMART CONTRACTS DESIGN

Smart Contracts	Explanations	Identities
MaterialRecord() *MaterialQuery()*	Record or query raw materials data	Producers, Collectors, Processors
ProductRecord() *ProductQuery()*	Record and query food product data	Processors, Sellers, Consumers
SignatureSign() *SignatureVerify()*	Each organization can use it to create a certificate and verify others	All
TransportationRecord()	Record the transportation details	Transporters
TransportationQuery()	Public transportation information are available for all	All
ManageTransactions()	Managers can make some operations on transactions on consortium blockchain	Managers

E. Blockchain Layer

As we progress to the exploration of the blockchain layer, we embark on a detailed examination of its core components. This layer is the technological bedrock that supports the entire supply chain ecosystem, ensuring the integrity, security, and efficiency of all transactions and data exchanges.

1) Blockchain Network: The design of the blockchain network is paramount, as it creates a robust, scalable, and interoperable system that caters to the unique demands of the agricultural food supply chain. The network is meticulously architected to accommodate the diverse needs of various stakeholders, from producers to consumers, while ensuring that the system remains secure and resistant to fraudulent activities.

Adhering to the traditional design principles of consortium blockchains, our approach similarly employs Public Key Infrastructure (PKI) as the cornerstone for member identity management and verification within the blockchain network. This foundation provides essential services such as certificate issuance and user authentication. By encapsulating the interactions, rules, and processes between members in a modular framework, we significantly streamline the costs associated with management, maintenance, upgrades, and updates, while concurrently enhancing operational efficiency. Such a system is particularly well suited for the complex dynamics of the agri-food supply chain. When an organizational node seeks to join the consortium blockchain network, it is initially required to provide validation information such as personal identification, employment details, and company credentials. Subsequently, the member management module assigns an identity to the node. Based on this identity information, the node can generate a pair of public and private keys, which are then utilized for a variety of operations within the blockchain network. This process ensures a secure and authenticated entry into the system, laying the groundwork for transparent and accountable interactions among all participants.

From the view of the blockchain network, sharding technology is a pivotal component designed to address the scalability challenges inherent in traditional blockchain networks. By implementing sharding, our system effectively partitions the blockchain into smaller, more manageable pieces, each capable of processing transactions independently. This approach not only enhances the overall transaction throughput but also reduces the computational burden on individual nodes. Each shard operates with its own consensus mechanism, allowing for parallel processing of transactions, which is crucial for maintaining high performance even as the network grows.

2) Sharding Blockchain: In the context of a consortium blockchain system that leverages sharding technology, a comprehensive blockchain ledger is tasked with documenting two distinct categories of information: transactions confined within individual shards, known as intra-shard transactions, and transactions that span across different shards, referred to as inter-shard transactions. Given the inherent access control and permission management attributes of consortium blockchains and features of agri-good supply chain, our system adopts a streamlined account/balance model, paving the way for the realization of more sophisticated states, including the deployment of smart contracts, thus providing a foundation for potential future advancements.

Similar to existing sharding systems, our system adopts the classic PBFT as intra-shard consensus protocol, and incorporates the BrokerChain mechanism for the facilitation of inter-shard transactions. BrokerChain is a sharding protocol designed to enhance the scalability of blockchain systems through state sharding. It operates in epochs, utilizing a combination of mining shards (M-shards) for transaction block generation and a partition shard (P-shard) for adaptive account state partitioning. This approach aims to balance the workload across shards and reduce inter-shard transactions. BrokerChain employs broker accounts to facilitate inter-shard transactions, ensuring their atomicity through a mechanism that involves creating and confirming two halves of a transaction. The workflow of BrokerChain mechanism is as shown in Fig. 6.

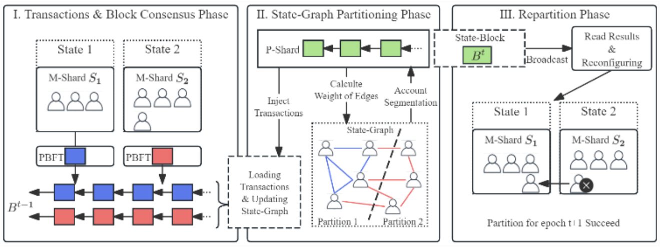

Fig. 6. BrokerChain-Workflow

The BrokerChain mechanism, while innovative, was initially tailored for public blockchain networks, therefore when it is adapted for consortium blockchains, several limitations become evident:

- Permissioned Environment: Consortium blockchains function within a permissioned environment, where all participants are recognized and authenticated. The sharding approach of the BrokerChain protocol does not fully capitalize on this, potentially resulting in a less-than-optimal distribution of transactions.

- Privacy Concerns: In a consortium context, privacy is a critical concern. The sharding mechanism of the BrokerChain protocol may not offer sufficient privacy controls, risking the exposure of sensitive transaction data to unauthorized nodes within the same shard.

- Scalability and Performance: Current sharding protocols in consortium blockchain may be impeded by the necessity for extensive inter-shard communication, potentially suffering redundant latency and diminishing throughput.

Understanding these limitations, WCLPA is crafted to transcend them, offering a solution more attuned to consortium blockchains. It integrates organization-based weighting and additional enhancements, aligning more closely with the structured and permissioned nature of consortium blockchain environments, and ultimately striving to provide a more efficient and secure sharding mechanism. The design of WCLPA will be introduced detailly in next section.

3) *Data Storage:* Our system's approach to data storage is underpinned by a combination of on-chain and off-chain storage mechanisms, optimized for efficiency, security, and accessibility. On-chain storage is pivotal, serving as the immutable ledger where all critical intra and inter transaction data and key supply chain events are permanently recorded. This ensures that every action within the network is traceable and verifiable, providing a foundation for trust and accountability. By anchoring hashes of off-chain data within this ledger, we maintain a clear link between the blockchain and its extended data ecosystem, thus preserving the integrity and continuity of the supply chain record.

Off-chain storage plays a complementary role, designed to handle the vast amounts of data generated by the supply chain, such as sensor logs and document archives. This data, while less critical for the immediate consensus process, is invaluable for detailed analysis and long-term planning. By storing this data in secure, encrypted data lakes, we ensure its confidentiality and integrity, with the added benefit of reducing the load on the blockchain network. The use of APIs facilitates controlled access to this data, enabling stakeholders to retrieve and analyze it as needed without compromising the blockchain's performance.

Furtherly, the hybrid nature of our storage model is further enhanced by the implementation of a hash linking mechanism, where the hashes of off-chain data are stored on-chain, creating a secure and efficient bridge between the on-chain and off-chain realms. This approach not only optimizes storage efficiency but also ensures that the data remains an integral part of the blockchain's verifiable history. The system is designed with scalability in mind, allowing for the dynamic adjustment of storage resources in response to the evolving demands of the agri-food supply chain. This future proofing strategy ensures that our blockchain network remains robust and adaptable, capable of supporting the industry's growth and technological advancements.

F. *Proposal of WCLPA*

To enhance the efficiency of a consortium blockchain system that supports the agri-food supply chain, our algorithm takes into account the inter-node relationships within the supply chain, assigning weights to transactions based on both transaction frequency and the organizational affiliation of the transacting parties, primarily their address information. By integrating role-based weighting into the sharding process, WCLPA aims to optimize the distribution of transactions across shards, thereby reducing latency, the ratio of cross-shard transactions, and improving throughput. The principles of WCLPA are as follows:

1) *Frequency and Organization-Based Weighting:* The algorithm considers both the frequency of transactions and the organizational affiliation of the transacting parties. In the agri-food supply chain system we have constructed, the flow of transactions and data is primarily aligned with the production and sales lifecycle of food products, from production to consumption. High-frequency transactions, such as those between producers and collectors or sellers and consumers, are given greater weight due to their regularity and the volume of data they generate. However, there are real-world scenarios where frequency as the only weight fails, such as multinational companies that only engage in import and export transactions, where the participating parties may experience high network latency and even time differences. Conversely, focusing solely on organizational identity as sharding weight factor may lead to inefficiencies when nodes within an organization frequently engage in transactions with nodes from other organizations, such as a merchant procuring or distributing goods in a different location. In such scenarios, these nodes are less

likely to be assigned to the same shard, hindering more efficient processing.

Therefore, it is imperative to concurrently consider both the frequency of transactions and the geographical distance between transacting parties, with the latter being ascertained through address information provided by organizational identities. Considering these situations, in our system model within a supply blockchain organized by region, transactions within the same organization should be assigned with greater weight, as most transactions occur within a unified organization, and such nodes are more physically and network-proximate, effectively reducing transaction latency and enhancing system performance. By combining these two types of weights, the partitioning of such a consortium blockchain network can be more efficient and accurate.

2) Transactions Load Balancing: When employing sharding techniques, a critical consideration is the balance between the volume of inter-transactions and the overall distribution of transactions. Sharding algorithms based on LPA method may lead to the formation of a large shard with a multitude of nodes. While this significantly reduces inter-shard transactions and can also lead to an imbalance in the overall distribution. This imbalance, in turn, may adversely affect system performance. In WCLPA, we have implemented a penalty mechanism for sharding feature weights to maintain a delicate balance between the number of inter-shard transactions and the overall transaction distribution, thereby enhancing the overall performance of the system.

Considering above two principles, organizations within the consortium blockchain are assigned with an address sequence. When transactions occur, the difference in the organizational sequence of the transacting parties is incorporated into the weight considerations. Assuming the difference in sequence between the transaction parties is denoted as d, a larger weight W_{seq} based on d indicates a higher probability of physical and network proximity and the potential for being assigned to the same shard. Conversely, a lesser value of W_{seq} implies that the parties involved in the transaction are less likely to be allocated to the same shard, and thus should be assigned a lower weight, aligning with the practical application scenarios of the agri-food supply chain system.

Within the LPA framework, we present the WCLPA design, which harnesses the dual nature of consortium blockchains and supply chains by integrating a frequency and organization-based weighting mechanism. Let the consortium blockchain system encompass M organizations, denoted as $[M] = \{1, 2, \dots, M\}$, with each organization O assigned a sequential location identifier m in the supply chain, where $m \in [M]$. The account network is represented as $G(V, E)$, with V representing a set of N accounts, denoted as $[N] = \{1, 2, \dots, N\}$, and E representing the set of edges interlinking these accounts. We utilize $[S] = \{1, 2, \dots, S\}$ to denote the set of S shards. For each account $i \in [N]$ affiliated with organization O_i, the corresponding address sequence is labeled as_i. Then we introduce a binary variable $x_{i,s}, s \in [S]$, to indicate the sharding partition outcome for an account. If x_i is assigned to shard s then $x_{i,s} = 1$, or else $x_{i,s} = 0$. Then we define $X = \{x_{i,s}, i \in [N], s \in [S]\}$as the comprehensive account partition solution for all accounts.

To be addressed, each account i can only be assigned to exactly one shard. Then we use $c_{i,j} \geq 0, i, j \in [N]$ to denote the count of transactions associated with account i and j, which comes as the first frequency weighting factor. Then we denote the second organization-based weight between account i and j as $w_{i,j}$, and use Gaussian function to normalize it as:

$$w_{i,j} = e^{-\frac{(as_i - as_j)^2}{2\lambda^2}} \tag{1}$$

Then we can use the weighting factor to calculate the ultimate weight $W_{i,j}$ of edge between account i and j:

$$W_{i,j} = c_{i,j} \cdot w_{i,j} \tag{2}$$

The utilization of the Gaussian function in the calculation of role weights is attributed to its smoothing properties, which facilitate a gradual transition in weight assignment, mitigating the impact of extreme values and thereby ensuring a more stable and continuous distribution of weights. The bell-shaped curve characteristic of the Gaussian function enables a rapid decay in weights between roles that are distant (or dissimilar), highlighting transaction relationships between organizations that are geographically or positionally close within the supply chain. Additionally, the Gaussian function serves as a filter to diminish the influence of random noise on weight calculations, particularly addressing anomalies or noise present in transactional data. It balances the impact of local (proximal nodes) and global (distal nodes) information, which is crucial for distributed decision-making processes within blockchain networks. By adjusting the parameters of the Gaussian function, such as λ, the weight distribution can be adapted flexibly to various network structures and transaction patterns, tailoring the allocation to the specific supply chain environment.

WCLPA accepts blockchain network $G(V, E)$, the maximum time of iterations τ and the threshold for update frequency ρ as inputs and outputs the shard partition results $V_1, V_2, \dots, V_S$ where $V_s (s \in [S])$ denotes the set of account addresses assigned to shard s. In initialization phase, the partition label $l(i)$ of vertex $i \in [N]$ is assigned an initial value according to its current shard. Subsequently, each vertex traverses its neighbors and computes a new partition label score through function $Score(i,s)$. We use $NV(i)$ to represent the neighbor vertexes of i and $LS(i) = \{l(j), j \in NV(i)\}$ to denote the label set. For each iteration, the new label of vertex i is represented by $\arg\max_{s\in[S]} S\,core(i,s)$. The score function is then defined as follows:

$$Score(i,s) = \sum_{j\in NV(i)} \frac{W_{i,j} \cdot \delta(l(j),s)}{\sum_{h\in NV(i)} W_{i,h}} \left(e^{-\beta\cdot\left(W_s - \min_{h\in[S]} W_h\right)}\right), \quad i \in [N], s \in LS(i) \tag{3}$$

The function $\delta(l(j),s)$ serves as an indicator, which is activated under the condition that $l(j) = s$ (i.e., when the partition result of account j is equal to s), yielding a value of 1; otherwise, it is nullified to 0. In addition, $W_s\left(s \in LS(i)\right)$ denotes the total weight of edges associated with shard s. Parameter $\beta \in [0,1]$ operates as a modifiable coefficient that gauges the punitive measure applied to the edge weight of shard s. A lower β leads to lower inter-shard transactions workload but a higher overall imbalance. In instances where a community's designation corresponds to a substantial size, the algorithm is capable of assigning a diminished score, thereby curtailing the magnitude of this community. The WCLPA persists in its iterative execution, independent of whether convergence is achieved within a predefined threshold of τ iterations. Each vertex is accorded the privilege to revise its label a maximum of ρ times. And the computing complexity of WCLPA is $O(N \cdot \tau)$.

THEORETICAL ANALYSIS

G. System Security

The application layer of proposed system is pivotal for the agri-food supply chain, meticulously managing interactions among various stakeholders such as raw material producers, collectors, processors, and transporters. It is equipped with a comprehensive member management system that bolsters traceability from production to consumption. The application layer is fortified by smart contracts that are not only integral to the system's operations but also significantly enhance its trustworthiness and automation. The organizational member management, transaction model, and smart contract design are all components that contribute to a secure and efficient application layer, ensuring that all interactions are authenticated and authorized.

Respectfully, the blockchain layer provides a secure and scalable infrastructure for the supply chain ecosystem. It is responsible for the execution of transactions and data storage. The security of this layer is underpinned by the BrokerChain Mechanism. Operating in epochs, it leverages mining shards (M-shards) for transaction block generation and a partition shard (P-shard) for dynamic account state partitioning, thereby balancing the workload and reducing inter-shard transactions. The security of M-shard is contingent upon the hash power distribution, with the probability of a node being malicious calculated based on the hash power of honest nodes and malicious nodes, and their respective mining focus. The system encourages honest nodes to participate in the PoW-based identity setup for both M-shard and W-shard to bolster the security of M-shard. The PBFT consensus protocol ensures fault tolerance, allowing the system to withstand Byzantine faults and maintain a high level of security.

H. Performances

The theoretical framework for the performance enhancement in our system is primarily anchored in the WCLPA, which operates iteratively, regardless of whether convergence is achieved within a specified number of iterations τ. Each vertex is permitted to update its label up to ρ times, contributing to the dynamic and adaptive nature of the sharding process. The computational complexity of the WCLPA is $O(N \cdot \tau)$, indicating a scalable approach to managing large scale networks. The iterative nature of WCLPA ensures that the sharding process continually refines itself, leading to a more balanced distribution of nodes across shards. This balance is crucial for reducing the computational burden on any single shard, thereby minimizing the risk of performance bottlenecks.

Theoretically, WCLPA algorithm offers several advantages over CLPA or LPA in the context of a agri-food supply chain. Firstly, the weighting design allows for a more granular control over the sharding process, ensuring that critical nodes are not overburdened and that the transaction load is distributed in a manner that reflects the real-world dynamics of the supply chain. Secondly, the WCLPA algorithm's iterative and adaptive nature ensures that the system can respond to changes in the network's structure and participant interactions, maintaining an optimal sharding configuration over time and achieving a higher degree of automation, trustworthiness, and efficiency in managing the complex dynamics of the agri-food supply chain.

EXPERIMENTS

I. Implementation on BlockEmulator

To validate the effectiveness of our proposed system and the performance of WCLPA, we implemented it in the BlockEmulator environment, selected for its unique support for verifying blockchain sharding mechanisms. This platform is equipped to handle the intricacies of intra-shard consensus, inter-shard committee organization, consensus algorithms, transaction processing, and communication protocols, which are often overlooked in conventional simulators. BlockEmulator's integration of recognized inter-shard consensus protocols provide a solid foundation for assessing the performance of our sharding-based system. The operational flow of BlockEmulator is depicted in Fig. 7.

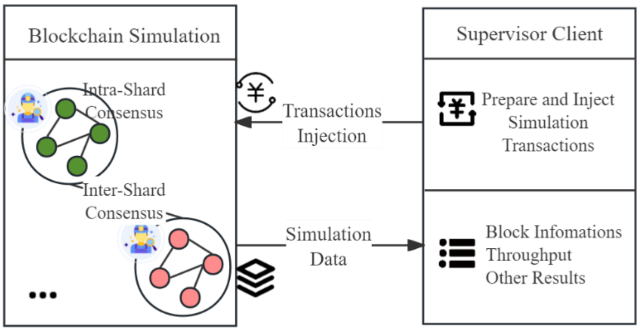

Fig. 7. BlockEmulator-Workflow

The core procedures of WCLPA we implemented are as shown in following Algorithm 1.

Algorithm 1 WCLPA

```
procedure ComputeEdgesWeight($NetGraph$)
    $EdgesWeight \leftarrow$ initialize array of size $ShardNum$
    for all edges $(u, v)$ in $NetGraph.WeightedEdgeSet$ do
        if $PartitionMap[u] \neq PartitionMap[v]$ then
            Increment inter-shard edge count for $PartitionMap[v]$
        end if
    end for
    Update minimum edge count and total inter-shard edge count
end procedure
procedure GetShardScore($v$, $shardN$)
    Calculate $EdgesWeight$ for vertex $v$ putting in $shardN$
    $score \leftarrow$ Edges connecting $v$ in $shardN$ / out-degree of v ×
        exp $(-WeightPenalty \times (EdgesWeight - MinEdgesWeight))$
    return $score$
end procedure
procedure Partition($NetGraph$)
    $ComputeEdgesWeight(NetGraph)$
    for $iter$ from 0 to $MaxIterations - 1$ do
        for all vertices $v$ in $NetGraph.VertexSet$ do
            Compute neighbor shard scores using GetShardScore($v$, $\cdot$)
            Find shard with maximum score $MaxScoreShard$
            if maximum score shard is different from current shard then
                1. Move vertex $v$ to $MaxScoreShard$
                2. Update partition map and vertex counts
                3. Recompute affected shard parameters
            end if
        end for
    end for
    return final partition and inter-shard edge count
end procedure
```

After implementation of WCLPA, its performance was evaluated within the BlockEmulator, especially comprising with CLPA of BrokerChain to demonstrate advantages when coming to consortium blockchain scenarios. The dataset utilized for this evaluation consisted of actual Ethereum transaction data, which served as the primary source of raw data. Each transaction was assigned a random address sequence marker. The algorithm's parameters were configured as follows: the penalty coefficient, denoted by β, was set to a default value of 0.5, while the maximum number of iterations τ, and the maximum number of label updates ρ, were defaulted to 100 and 50, respectively. For each block, the transaction cap was set at 2000. Within the shard, the PBFT consensus protocol was configured with a consensus delay of 10 seconds, and the duration of each epoch was established at 100 seconds. And to ensure the precision, the experimental procedure will be executed over a span of 10 epochs, with the average value of these iterations being adopted as the definitive outcome of the experiment.

RESULTS

J. Transactions Per Second

Comparisons of TPS between our scheme and original CLPA of BrokerChain is depicted in Fig. 8. The results demonstrate that the throughput of our scheme outperforms. Especially as the number of shards increases, there is a tendency for a decline in TPS of CLPA, whereas our scheme continues to demonstrate a positive enhancement in performance. This improvement is attributed to the refined weight distribution strategy and the incorporation of role-based and proximity-based factors in the sharding process, which contribute to the enhanced efficiency and scalability of the blockchain system. Moreover, as the number of shards and nodes increases, the throughput also escalates, thereby showcasing the scalability of our scheme.

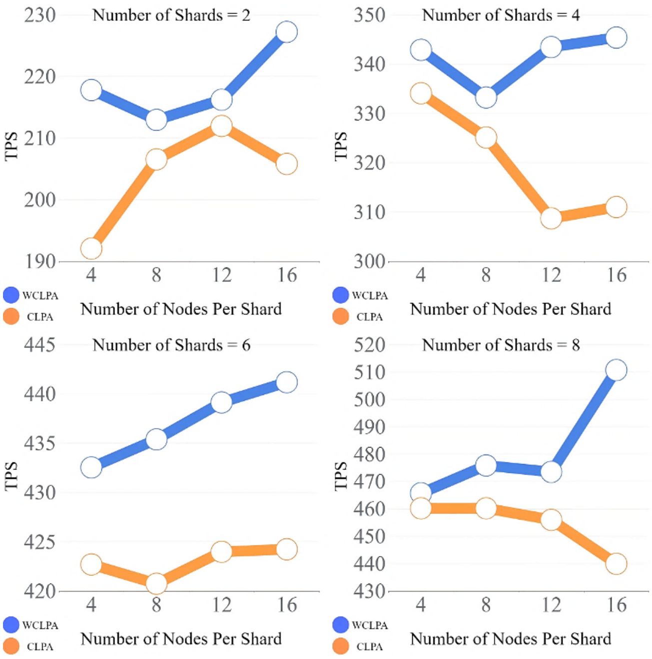

Fig. 8. TPS Comparison

K. Confirmation Time

We examined the transaction confirmation time as showed in Fig. 9. Notably, WCLPA significantly outperforms the CLPA in this regard, with a confirmation time that is approximately 1/3 to 1/4 of the latter. This substantial reduction in confirmation time indicates a marked improvement in our system's latency, network stability, and resilience to disturbances. The superior sharding rules in our algorithm contribute to these enhancements, reflecting an optimized distribution and processing of transactions across the blockchain network. Also, as the number of shards increases, the confirmation time decreases since the overall transactions are distributed in a more balanced way, thereby showcasing the scalability of our scheme.

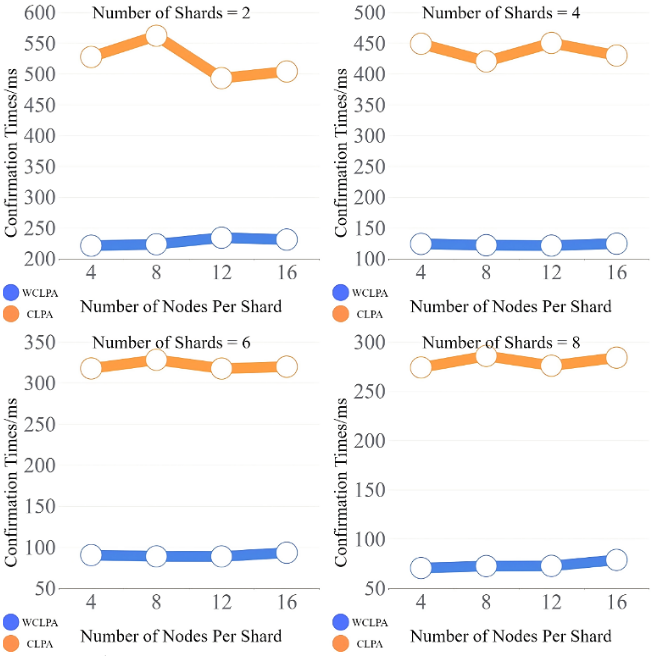

Fig. 9. Confirmation Time Comparison

L. *Inter-Shard Ratio*

Finally, we assessed the inter-shard transaction ratio. It is important to note that a higher proportion of inter-shard transactions implies a lower proportion of intra-shard transactions, which typically correlates with superior system performance. From the results depicted in the accompanying Fig. 10, it is evident that WCLPA consistently delivers a lower rate of inter-shard transactions. This reduction effectively enhances the load balance and overall performance of the system by promoting a higher frequency of intra-shard transactions, thereby optimizing the utilization of shard resources and streamlining transaction processing.

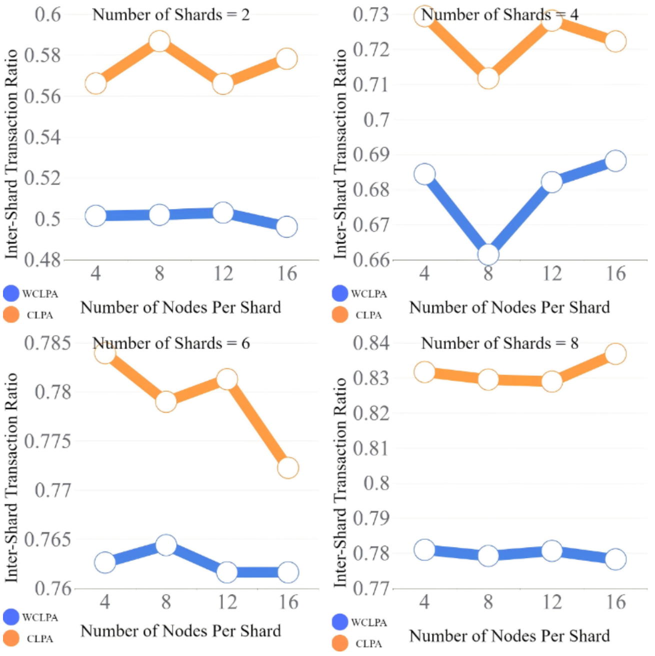

Fig. 10. Inter-Shard Transaction Ratio Comparison

CONCLUSION

Our comprehensive experiments results reveal the distinct advantages of the WCLPA in various critical performance metrics when occurring to consortium blockchain scenarios within our proposed agri-food supply chain system. Our scheme accomplishes a superior throughput of system and maintains a positive enhancement with increasing number of shards. This improvement is primarily due to the refined weight distribution strategy and the integration of frequency and proximity-based factors in the sharding partitioning process, which significantly enhance the efficiency and scalability of the blockchain system. Furthermore, our scheme achieves a significantly lower transaction confirmation time, approximately 1/3 to 1/4 of that required by CLPA, indicating a substantial improvement in system latency, network stability, and resilience to disturbances. Additionally, WCLPA consistently provides a lower rate of inter-shard transactions, which, by promoting a higher frequency of intra-shard transactions, effectively optimizes resource utilization and streamlines transaction processing. Collectively, these results underscore the robust performance, scalability and load balancing of our scheme, positioning it as a formidable solution for enhancing blockchain systems.

REFERENCES

[1] K. Li, J.-Y. Lee, and A. Gharehgozli, “Blockchain in food supply chains: a literature review and synthesis analysis of platforms, benefits and challenges,” International Journal of Production Research, vol. 61, no. 11, pp. 3527–3546, Jun. 2023, doi: 10.1080/00207543.2021.1970849.

[2] Q. Lu and X. Xu, “Adaptable Blockchain-Based Systems: A Case Study for Product Traceability,” IEEE Software, vol. 34, no. 6, pp. 21–27, Nov. 2017, doi: 10.1109/MS.2017.4121227.

[3] M. Nakasumi, “Information Sharing for Supply Chain Management Based on Block Chain Technology,” in 2017 IEEE 19th Conference on Business Informatics (CBI), Jul. 2017, pp. 140–149. doi: 10.1109/CBI.2017.56

[4] N. Vu, A. Ghadge, and M. Bourlakis, “Blockchain adoption in food supply chains: a review and implementation framework,” Production Planning & Control, vol. 34, no. 6, pp. 506–523, Apr. 2023, doi: 10.1080/09537287.2021.1939902.

[5] N. Friedman and J. Ormiston, “Blockchain as a sustainability-oriented innovation?: Opportunities for and resistance to Blockchain technology as a driver of sustainability in global food supply chains,” Technological Forecasting and Social Change, vol. 175, p. 121403, Feb. 2022, doi: 10.1016/j.techfore.2021.121403.

[6] H. Huang et al., “BlockEmulator: An Emulator Enabling to Test Blockchain Sharding Protocols,” Nov. 11, 2023, arXiv: arXiv:2311.03612. doi: 10.48550/arXiv.2311.03612.

[7] Feng Tian, "A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things," 2017 International Conference on Service Systems and Service Management, Dalian, 2017, pp. 1-6, doi: 10.1109/ICSSSM.2017.7996119.

[8] Z. Li, H. Wu, B. King, Z. Ben Miled, J. Wassick, and J. Tazelaar, “A Hybrid Blockchain Ledger for Supply Chain Visibility,” in 2018 17th International Symposium on Parallel and Distributed Computing (ISPDC), Jun. 2018, pp. 118–125. doi: 10.1109/ISPDC2018.2018.00025.

[9] F. Antonucci, S. Figorilli, C. Costa, F. Pallottino, L. Raso, and P. Menesatti, “A review on blockchain applications in the agri-food sector,” J Sci Food Agric, vol. 99, no. 14, pp. 6129–6138, Nov. 2019, doi: 10.1002/jsfa.9912.

[10] A. Shahid, A. Almogren, N. Javaid, F. A. Al-Zahrani, M. Zuair, and M. Alam, “Blockchain-Based Agri-Food Supply Chain: A Complete

Solution," IEEE Access, vol. 8, pp. 69230–69243, 2020, doi: 10.1109/ACCESS.2020.2986257.

[11] A. Kamilaris, A. Fonts, and F. X. Prenafeta-Boldύ, "The rise of blockchain technology in agriculture and food supply chains," Trends in Food Science & Technology, vol. 91, pp. 640–652, Sep. 2019, doi: 10.1016/j.tifs.2019.07.034.

[12] P. Karthik and T. Vamshi Krishna, "To Enhance Enterprise Resource Planning with Blockchain: Food Supply Chain," IJSR, vol. 11, no. 4, pp. 277–283, Apr. 2022, doi: 10.21275/SR22401220948.

[13] R. AlTawy, M. ElSheikh, A. M. Youssef, and G. Gong, "Lelantos: A Blockchain-Based Anonymous Physical Delivery System," in 2017 15th Annual Conference on Privacy, Security and Trust (PST), Aug. 2017, pp. 15–1509. doi: 10.1109/PST.2017.00013.

[14] K. Toyoda, P. T. Mathiopoulos, I. Sasase and T. Ohtsuki, "A Novel Blockchain-Based Product Ownership Management System (POMS) for Anti-Counterfeits in the Post Supply Chain," in IEEE Access, vol. 5, pp. 17465-17477, 2017, doi: 10.1109/ACCESS.2017.2720760.

[15] H. R. Hasan and K. Salah, "Blockchain-Based Proof of Delivery of Physical Assets With Single and Multiple Transporters," in IEEE Access, vol. 6, pp. 46781-46793, 2018, doi: 10.1109/ACCESS.2018.2866512.

[16] H. Dang, T. T. A. Dinh, D. Loghin, E.-C. Chang, Q. Lin, and B. C. Ooi, "Towards Scaling Blockchain Systems via Sharding," in Proceedings of the 2019 International Conference on Management of Data, in SIGMOD '19. New York, NY, USA: Association for Computing Machinery, Jun. 2019, pp. 123–140. doi: 10.1145/3299869.3319889.

[17] M. Zamani, M. Movahedi, and M. Raykova, "RapidChain: Scaling Blockchain via Full Sharding," in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, in CCS '18. New York, NY, USA: Association for Computing Machinery, Oct. 2018, pp. 931–948. doi: 10.1145/3243734.3243853.

[18] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A Secure Sharding Protocol For Open Blockchains," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna Austria: ACM, Oct. 2016, pp. 17–30. doi: 10.1145/2976749.2978389.

[19] G. Yu, X. Wang, K. Yu, W. Ni, J. A. Zhang and R. P. Liu, "Survey: Sharding in Blockchains," in IEEE Access, vol. 8, pp. 14155-14181, 2020, doi: 10.1109/ACCESS.2020.2965147

[20] E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, E. Syta and B. Ford, "OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding," 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2018, pp. 583-598, doi: 10.1109/SP.2018.000-5.

[21] H. Huang et al., "BrokerChain: A Cross-Shard Blockchain Protocol for Account/Balance-based State Sharding," May 2022. doi: 10.1109/INFOCOM48880.2022.9796859.

[22] C. Li et al., "Achieving Scalability and Load Balance across Blockchain Shards for State Sharding," Sep. 2022. doi: 10.1109/SRDS55811.2022.00034.

[23] "Community detection with the Label Propagation Algorithm: A survey," Physica A: Statistical Mechanics and its Applications, vol. 534, p. 122058, Nov. 2019, doi: 10.1016/j.physa.2019.122058.

[24] C. Tong, J. Niu, J. Wen, Z. Xie, and F. Peng, "Weighted label propagation algorithm for overlapping community detection," in 2015 IEEE International Conference on Communications (ICC), Jun. 2015, pp. 1238–1243. doi: 10.1109/ICC.2015.7248492.

[25] G. B. da Fonseca, G. Sargent, R. Sicre, Z. K. G. Patrocínio, G. Gravier, and S. J. F. Guimarães, "Hierarchical multi-label propagation using speaking face graphs for multimodal person discovery," Multimed Tools Appl, vol. 80, no. 2, pp. 2797–2820, Jan. 2021, doi: 10.1007/s11042-020-09692-x.