electronics

MDPI

Article

A Cross-Institution Information-Sharing Scheme Based on a Consortium Blockchain

Bingbing Tan [1], Yanli Chen [1,*], Yonghui Zhou [1], Shouqing Li [2] and Zhicheng Dong [3]

[1] School of Big Data and Computer Science, Guizhou Normal University, Guiyang 550025, China; 21010230688@gznu.edu.cn (B.T.); yonghuizhou@gznu.edu.cn (Y.Z.)
[2] Key Laboratory of Flight Techniques and Flight Safety, CAAC, Guanghan 618307, China; soulea@163.com
[3] School of Information Science and Technology, Tibet University, Lhasa 850000, China; dongzc666@163.com
* Correspondence: yanli_027@gznu.edu.cn

Abstract: In today's data-driven world, efficient and secure cross-institution information-sharing is an urgent challenge. Traditional information-sharing methods based on access controlling often suffer from issues such as privacy breaches and high communication complexity. To address this issue, this paper proposes a cross-institution information-sharing solution based on a consortium blockchain, in which it combines on-chain transaction consensus with off-chain institution storage, thereby facilitating collaboration among nodes from different institutions on the blockchain. To enhance the efficiency and security of transactions on the blockchain, we also introduce a dynamic and adaptive Practical Byzantine Fault Tolerance (DA-PBFT) consensus protocol, which permits nodes to dynamically join and exit the blockchain network, consequently improving network scalability. Through a reputation mechanism, we swiftly identify and remove faulty and malicious nodes, enhancing the trustworthiness of nodes in the information-sharing network based on consortium blockchain, thereby improving consensus efficiency. We have also employed encryption techniques to enhance the privacy and integrity of data during the process of cross-institution information sharing. A comprehensive analysis of the communication complexity in the information-sharing network confirms the effectiveness and security of our proposed solution. We offer a unique solution to improve the efficiency and security of cross-institution information-sharing while ensuring data integrity and privacy. By addressing the challenges of privacy breaches and high communication complexity in information sharing, we establish a foundation for secure cross-institution data exchange.

Keywords: consortium blockchain; cross-institution information-sharing; adaptive consensus; PBFT

Citation: Tan, B.; Chen, Y.; Zhou,Y.; Li, S.; Dong, Z. A Cross-Institution Information-Sharing Scheme Based on a Consortium Blockchain. *Electronics* **2023**, *12*, 4512. https://doi.org/10.3390/electronics12214512

Academic Editor: Rameez Asif

Received: 28 September 2023
Revised: 23 October 2023
Accepted: 31 October 2023
Published: 2 November 2023

1. Introduction

In an age characterized by the growing dependence on data, the imperatives of security and efficiency in inter-institution information sharing have attained unprecedented significance. Nevertheless, conventional approaches to information sharing are beset with challenges privacy breaches and high communication complexity. Consequently, there is an urgent demand for a secure and highly efficient means of information sharing.

In 2008, Satoshi Nakamoto [1] introduced blockchain technology, which boasts attributes of being distributed, tamper-proof, and traceable. In contrast to conventional information-sharing methods, blockchain-based solutions for information sharing ensure that data are consistently stored on the chain. This not only breaks down information barriers, but also prevents unauthorized access, providing technical assurance for inter-institution information-sharing. For the information-sharing methods based on blockchain, Chen et al. [2] proposed a framework for establishing authenticated personal information using blockchain, providing secure and tamper-proof storage for individuals' trusted certificates. However, this framework has limited security and lacks a rigorous certificate verification process. Aida Kamisalic et al. [3] introduced a student-centered information management solution based on blockchain, optimizing the certificate verification process.

Lizcano et al. [4] proposed an information sharing method that utilizes blockchain to record student skills and smart contracts for automatic certificate verification and confirmation, enhancing trust among students, training institutions, experts, and employers.

However, existing information sharing schemes [5–7] using public chains make the privacy of confidential or sensitive information insecurity. In contrast, consortium blockchains provide access control for a selected group of participants in [5]. In [6], consortium blockchains provide enhanced privacy and confidentiality through permission access [7], which are crucial for information sharing. Using consortium blockchains to share information has been paid more attention.

Furthermore, several methods [8–13] for information management using consortium blockchains have been proposed. Parminder Kaur et al. [8] introduced a framework to enhance the future employability of educators, incorporating a rewarding token system to incentivize continuous improvement of teachers' skills. Yang et al. [10] proposed a blockchain-based information management system, encrypting the original files, securely storing them in a segmented form on the InterPlanetaryFile System (IPFS), ensuring the integrity of the data. Zhao et al. [11] presented a blockchain-based information-sharing platform model, storing user permission information, resource aggregation information, and storage locations on the chain, using smart contracts to verify identity information, thereby enhancing information security and credibility. Wu et al. [12] introduced a blockchain-based smart healthcare system with fine-grained privacy protection for reliable data exchanging and sharing among different users. Yu et al. [13] built a multi-collaborative information-sharing mechanism based on blockchain, utilizing blockchain technology to achieve secure and efficient information sharing. However, the methods of information-sharing mentioned above emphasize interpersonal and intra-institutional information-sharing, lacking secure and efficient means of information-sharing between different institutions.

For consortium blockchains, the consensus protocol is one of the crucial factors affecting the overall efficiency of the information-sharing network. The traditional consensus is realized by multi-round voting with a three-phase protocol with high communication complexity, which was proposed as the Practical Byzantine Fault Tolerance (PBFT) protocol in 1999 [14]. Later, Andrew et al. [15] introduced an improved protocol called The Honey Badger of BFT Protocols based on PBFT, enhancing scalability and robustness. However, this protocol exhibits high communication complexity too. Yin et al. [16] presented Hotstuff, a protocol that achieves high throughput, low latency, and low communication complexity by utilizing a leader-based structure and a three-phase voting process. However, in highly asynchronous networks or scenarios with a large number of faulty nodes, it may experience failures. Duan et al. [17] proposed Foundations of Dynamic BFT, which relies on a configuration discovery sub-protocol to manage member requests. Due to the additional costs associated with the sub-protocol, this protocol exhibits high communication complexity too.

Within a blockchain network, consensus protocols with low communication complexity can significantly enhance the network's efficiency. Similarly, when consortium blockchain is employed in cross-institution information-sharing networks, the pursuit of low communication complexity remains of paramount importance. To address the security and efficiency challenges of cross-institution information-sharing, this paper proposes a cross-institution information-sharing scheme based on consortium blockchains. Additionally, we introduce a dynamic and adaptive PBFT consensus protocol to enhance the efficiency of the consensus protocol. The contributions in this paper are as follows:

- A cross-institution information-sharing scheme based on consortium blockchain is proposed, which enables the sensitive data of one institution privacy shared with others;
- A dynamic and adaptive PBFT consensus protocol is proposed. The security of the blockchain network has been enhanced by the utilization of a reputation mechanism to remove malicious nodes.

The rest of this paper is organized as follows. Section 2 provides an overview of the cross-institution information-sharing network based on a consortium blockchain. In

Section 3, the improved consensus protocol is introduced. Section 4 conducts a detailed performance analysis of the cross-domain information sharing network and, finally, Section 5 offers a comprehensive summary of the key findings presented in this paper.

2. The Proposed Cross-Institution Information-Sharing Network Based on a Consortium Blockchain

In cross-institution information-sharing networks, information sharing and privacy protection have always been topics of concern [18]. To achieve secure and efficient information exchange between multiple institutions, a delicate balance must be struck between two crucial aspects: safeguarding information privacy and enabling inter-institution information sharing. To achieve this nuanced balance, we employ intricate encryption techniques and consensus protocols, ensuring the confidentiality of private information while enhancing the consensus efficiency of the inter-institution information-sharing network.

The cross-institution information-sharing network based on consortium blockchain comprises multiple mutually trusted institutional alliances. As shown in Figure 1, it represents the framework of a cross-institution information-sharing network based on a consortium blockchain. The cross-institution information-sharing module in Figure 1 represents the process of encrypting shared information. We use zk-SNARKs [19] and proxy re-encryption [20] techniques for information encryption, thus ensuring the security and confidentiality of the data. We will provide a detailed explanation of the cross-institution information-sharing process in Section 2.1.

In the consensus module of Figure 1, different colored icons represent nodes belonging to different institutions. Each institution can have multiple nodes within the consortium blockchain. All of these nodes collectively participate in achieving consensus on the order and content of transactions within the network, which is subsequently recorded on the blockchain. Our enhanced DA-PBFT consensus protocol serves to improve the consensus efficiency of the information sharing network. (This is detailed in Section 3).

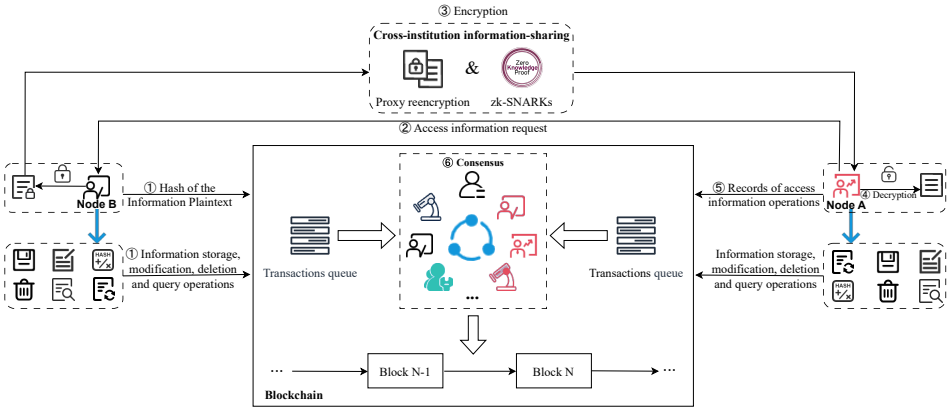

Figure 1. Diagram of the proposed cross-institution information-sharing network.

In this section, we describe our proposed method for cross-institution information-sharing based on consortium blockchain shown in Figure 1, which is realized with two parts, information storage and information sharing.

2.1. Information Storage

For a cross-institution information-sharing network, most data are stored off-chain by the nodes in their fixed regions, and only the digest and metadata, which includes operations, such as hashing values, recording sharing activities, storing information data, making modifications, conducting queries, and performing deletions, are stored in the blockchain after reaching consensus. Then, the nodes on the blockchain network can only acquire the digest and metadata. When they cannot acquire original private data on blockchain, they must acquire it in other ways. Storing metadata on-chain and information data off-chain

not only conserves space on the blockchain, but also safeguards the confidentiality of sensitive data.

Assume that the blockchain network consists of several institutional alliances representing different regions separately. For each institution, several nodes exist in the consortium blockchain. As shown in Figure 1, the different colors represent nodes from distinct institutions, and all these nodes will reach consensus about the order and transactions [21], and then stored them in the blockchain. To avoid the malicious and fault nodes in the blockchain, each operation for nodes will be scored according to their responsivity as their reputation values [22] to distinguish Byzantine nodes. In the context of a cross-institution information-sharing network based on consortium blockchain, the consensus protocol enables all nodes to achieve consensus on the order and content of transactions, establishing a shared, consistent distributed ledger to ensure the security and immutability of the blockchain.

2.2. Information Sharing

Generally, in a special region, the information is stored in a local area network and can be accessed freely. However, even nodes from different institutions exist within the same blockchain network, they cannot directly access data on the blockchain network.

To facilitate cross-institution sharing of private data within the blockchain network, we employ zk-SNARKs [19] and proxy re-encryption [20] technologies to ensure the privacy and security of shared information. zk-SNARKs [19] are utilized for encrypting and proving the validity of sensitive information. This means that various institutions can collectively verify the integrity and accuracy of sensitive data without exposing privacy details, maintaining a high degree of privacy and confidentiality. Proxy re-encryption technology is used to encrypt shared information, allowing institutions to securely share information without disclosing decryption keys. This implies that each institution can retain full control over its data while permitting authorized parties from other institutions to access the data when needed. By integrating zk-SNARKs [19] and proxy re-encryption [20] technologies into our information-sharing solution, we not only ensure data integrity and privacy but also simplify the complex process of inter-institution information-sharing.

As shown in Figure 1, Node A is aware of the types of information stored by Node B through the information storage records on the blockchain, he wishes to access this information as follows:

1. Node B stores the information hash and metadata on the blockchain (① in Figure 1);
2. Node A initiates a request to Node B (② in Figure 1);
3. Node B, based on Node A's access permissions, encrypts the shared information using zk-SNARKs [19] and proxy re-encryption [20] technology and then shares it with Node A (③ in Figure 1);
4. Node A decrypts the encrypted information using its private key, thereby gaining the required access rights. For sensitive information, we employ zk-SNARKs [19] to generate proofs of sensitive data (④ in Figure 1);
5. Node B can verify the content of sensitive data without needing access to the specific details of the sensitive information. After successful verification, Node B records the access as a transaction on the blockchain network, awaiting consensus (⑤ in Figure 1);
6. Nodes within the cross-institution information-sharing network collectively participate in reaching consensus on the order and content of transactions (⑥ in Figure 1), subsequently recording the transactions on the blockchain. The consensus protocol used by nodes to achieve consensus on transactions is the DA-PBFT consensus protocol proposed in this paper. We will provide a detailed introduction to this consensus protocol in Section 3.

3. Dynamic and Adaptive PBFT Consensus Protocol

Cross-institution information-sharing is inherently sensitive and requires a high degree of trust and security. Consortium blockchains, as distributed networks, mitigate the risk of

single points of failure. However, they are not immune to malicious actors. To ensure that cross-institution information-sharing networks can withstand adversarial behavior without compromising the integrity of shared information, Byzantine fault tolerance becomes imperative.

In the proposed blockchain-based cross-institution information-sharing network (Section 2), it is easy for tampers to pretend to be a legal nodes. To ensure the security of this cross-institution information-sharing network, we employ a consensus protocol to supervise the behaviors of the nodes. When a node exhibits abnormal behavior, its reputation value will subsequently be decreased. Once the reputation value of a node falls below a threshold, the node will be forced to logout from the network.

3.1. The PBFT Consensus Protocol

Miguel and Barbara [14] introduced PBFT in 1999 as a response to the challenge of achieving consensus among a group of nodes when Byzantine faults are present, encompassing malicious behavior and random node failures. PBFT addresses the critical issue of achieving consensus among nodes in a network, even in the presence of potential malicious or faulty nodes. This consensus is crucial for maintaining the integrity and immutability of a blockchain's distributed ledger, ensuring that all participants can agree on a common set of transactions and their order. PBFT is divided into three primary phases: pre-prepare, prepare, and commit, as shown in Figure 2.

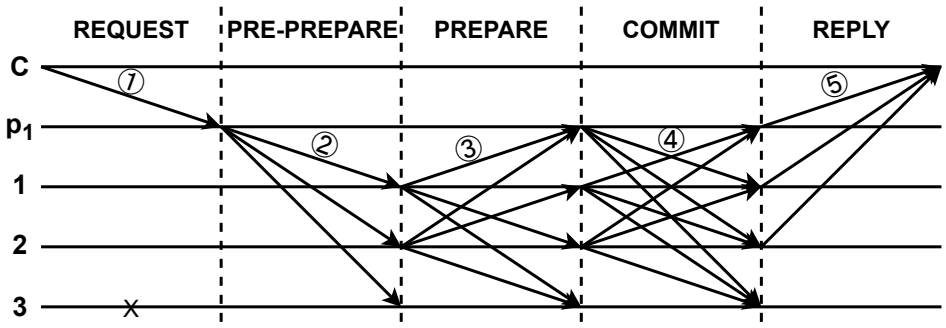

Figure 2. The process of PBFT [14].

One of PBFT's key strengths is its practicality and efficiency in achieving consensus, even in the presence of adversarial nodes. It can tolerate up to $(n-1)/3$ malicious nodes in a network of n nodes, making it particularly resilient and suitable for consortium blockchain applications where trust may be limited.

3.2. The Proposed Dynamic and Adaptive PBFT Consensus Protocol

PBFT provides several benefits for distributed systems, including fault tolerance, deterministic execution, and the finality of decisions. However, for one time consensus, any node cannot dynamically join and exit the blockchain network. Further, when a Byzantine node or redundant nodes exist in this network, it will result in high communication complexity and insecurity. Hence, a dynamic and adaptive PBFT consensus protocol is proposed to optimize the communication complexity guarantee the security of the blockchain network. The schematic of this protocol is shown in Figure 3.

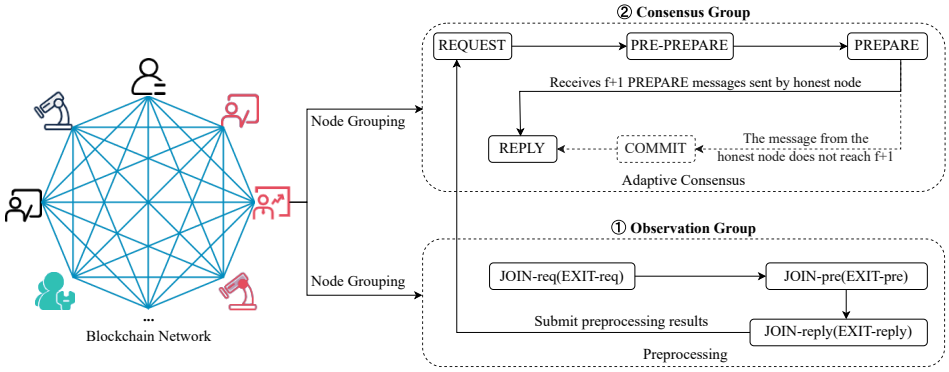

Figure 3. Diagram of the proposed dynamic and adaptive PBFT consensus protocol framework.

Firstly, nodes within the cross-institution information-sharing network based on consortium blockchain are randomly divided into consensus groups and observation groups. Assume that there are n nodes in the blockchain network. After randomly dividing them into groups, the consensus group consists of n_1 nodes, and the observation group consists of n_2 nodes.

$$n_1 = \left\lfloor \frac{n}{2} \right\rfloor \tag{1}$$

$$n_2 = n - \left\lfloor \frac{n}{2} \right\rfloor \tag{2}$$

where $n_1 > 4$, $n_2 > 4$, $n_1 + n_2 = n$.

We use r(r $\in$ [0,1]) to denote the reputation value to measure the honestness of nodes. Higher reputation values indicate more honestness. Initially, all nodes are given a reputation value of 0.5, including new nodes, and each node maintains a local node list (NL) including their identity number, IP address/port, public key, reputation value, and trusted state. After each round consensus, all nodes update their reputation values using the reputation model in [22]. Table 1 shows the definitions of the notations used in this paper.

Table 1. Definition of notations.

Nations	Descriptions
n	n is the number of the network blockchain
f	f is the number of faulty nodes
n_1	n_1 is the number of consensus nodes
n_2	n_2 is the number of observation nodes
p_1	Primary node of the consensus group
p_2	Primary node of the observation group
i	a new node's ID
j	a replica
pk	pk is the public key
σ_i	σ_i is the signature of node i
v	v is the current view number
m	m is the message to transmit
s	s is the message sequence number
d	d is the message m digest
|m|	|m| is the size of the client request message
C	C is the stable checkpoint

3.2.1. The Proposed Adaptive Consensus

In the cross-institution information-sharing network based on the consortium blockchain, a novel consensus mechanism with reputation model, enabling nodes within the consensus group to dynamically execute three-phase or two-phase consensus based on their respective reputation values. By adapting the consensus process according to the reputation of each participating node, we effectively streamline the communication complexity and enhance the overall efficiency of the consensus algorithm. Figure 4 illustrates the process of two-phase consensus.

The adaptive consensus mechanism is primarily used to address the dynamic joining and exiting of the blockchain network. When the reputation value of a node remains below a specific threshold for consecutive t rounds of consensus, the node will be considered illegitimate and forcibly removed from the blockchain network.

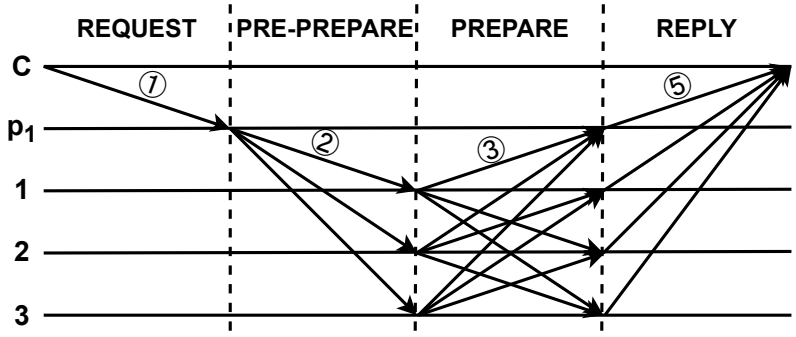

Figure 4. The process of two-phase consensus.

3.2.2. Nodes Join the Blockchain Dynamically

The nodes in the consensus group, are responsible for consensus on transactions, while the nodes in the observation group are to preprocessing requests to join the group. When a new node wants to join the blockchain, it will be processed as Figure 5, which consists of two stages, preprocessing requests to join the group from the nodes in the observation group, and the consensus phase.

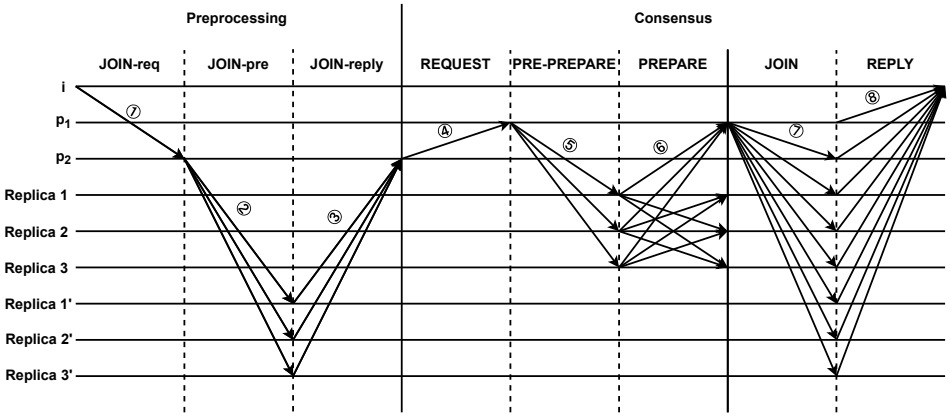

Figure 5. The process of a new node joining the blockchain.

1. The preprocessing requests phase.
   Assuming a new node i sends a request to join the blockchain (① in Figure 5), the preprocessing is applied as follows:
   (a) p_2 checks the identity information of node i. If the verification is successful, it sends a message < < JOIN-pre, v′, s′, d′>, m > σ_{p_2} to the replica nodes of the observation group (② in Figure 5). Otherwise, it discards the request message;
   (b) Upon receiving the JOIN-pre message, the replica nodes of the observation group validate the message by verifying the correctness of the signature and comparing the calculated hash of the message with its digest. If the validation is successful, the replica node sends an <JOIN-reply, v′, s′, j', D(m) > $\sigma_{j'}$ message to p_2 (③ in Figure 5). Otherwise, it discards the message;
   (c) When p_2 receives JOIN-reply messages with valid signatures from f+1 different replica nodes, it sends the preprocessed result as the consensus request message <REQUEST, o, t, c > σ_{p_2} to the nodes of the consensus group (④ in Figure 5). This ensures that the result is valid, as at most f replicas can be faulty.

2. The consensus phase.
The nodes in the consensus group only perform a two-phase consensus process, consisting of the pre-preparing and preparing phases. When the consensus group primary node p_1 receives a request message, it initiates a two-phase protocol, automatically broadcasting the request to the replica nodes of the consensus group:
   (a) p_1 assigns a sequence number s to the request and multicasts < < PRE-PREPARE, v, s, d > σ_{p_1}, m> to the replica nodes of the consensus group (⑤ in Figure 5);
   (b) Upon receiving the pre-preparing message, the replica nodes of the consensus group perform the following verification operations:
      - Check the signatures of the request and pre-preparing messages, and verify if d is the digest of m;
      - Check if it is in view v;
      - Check if it has not received a pre-preparing message with a different digest for the same v and s.

      If the replica nodes of the consensus group accept the pre-preparing message, it multicasts a <PREPARE, v, n, d, j > σ_j message to all other replica nodes of the consensus group (⑥ in Figure 5); otherwise, the replica node j does nothing;
   (c) The replica nodes of the consensus group accept preparing messages if the signatures are correct and their view number matches the current view v of the replica bodes. When a replica node of the consensus group receives preparing messages from $2f$ different replica nodes with high reputation values, p_1 broadcasts the message <JOIN, i, ip> to all nodes in the blockchain (⑦ in Figure 5);
   (d) The nodes in the blockchain synchronize messages and add the information of node i to the locally maintained NL table. Then, they send a reply message <REPLY, v, t, j, r, C, NL> to the new node i (⑧ in Figure 5);
   (e) When the new node i receives f + 1 reply messages from different nodes, it successfully joins the blockchain.

3.2.3. Nodes Exits the Blockchain Dynamically

There are two scenarios for a node to exit the blockchain: voluntary exiting and forced exiting. A node will be forcibly removed from the blockchain when its reputation value R is less than special threshold for consecutive t rounds to avoid malicious behavior or non-compliance. As shown in Figure 6, the illustration portrays the process of a node exiting the blockchain.

1. Voluntary exit.
A voluntary exiting from blockchain network is realized through two stages, preprocessing and consensus, as shown in Figure 6.

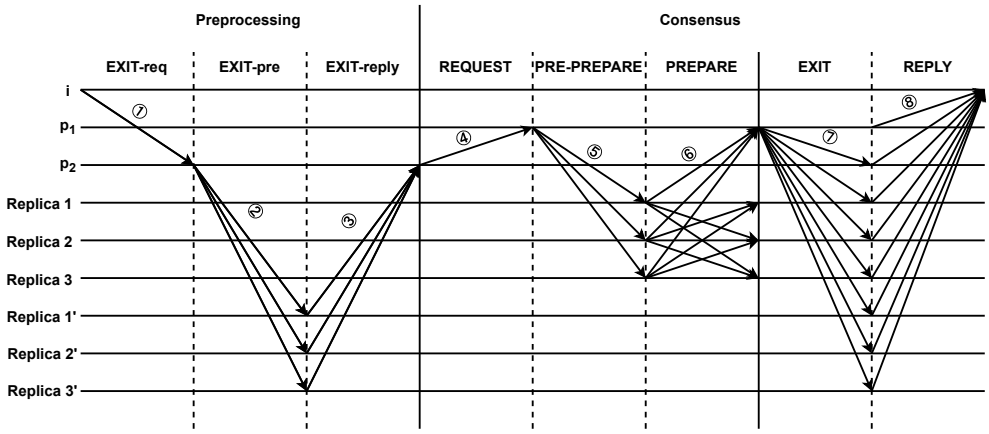

Figure 6. The process of a node exiting the blockchain.

(a) The preprocessing requests phase.
In the blockchain network, node i initiates exit request<EXIT-req, i, ip, pk, NL> to performs a preprocessing (① in Figure 6). The detailed process is as follows:

i. Receiving the EXIT-req request, p_2 first checks the node's view number and other information. Then, p_2 sends the < < EXIT-pre, v', s', d'>, m > σ_{p_2} message to the observing group's replica nodes (② in Figure 6);
ii. Receiving the EXIT-pre message, the observing group's replica node verifies the message by checking the correctness of the signature and comparing the message's hash with its digest. If the verification passes, the replica node sends <EXIT-reply,> to p_2 (③ in Figure 6);
iii. After receiving f+1 valid signatures of EXIT-reply messages from different replica nodes, p_2 includes the preprocessing node as part of the consensus group's request message <REQUEST, o, t, c > σ_{p_2}, which is then sent to the nodes of the consensus group (④ in Figure 6).

(b) The consensus phase.
Due to the introduction of a reputation model, the nodes in the consensus group can perform a two-phase consensus process, consisting of the pre-preparing and preparing phases. The complete process of consensus among the nodes in the consensus group is as follows:

i. Node i in the blockchain first send an exit request <REQUEST, o, t, c > σ_{p_2} (④ in Figure 6);
ii. When p_1 receives request message, it initiates a two-phase protocol to atomically broadcast the request to the replica nodes of the consensus group;
iii. p_1 assigns a sequence number s to the request and multicasts < < PRE-PREPARE, v, s, d > σ_{p_1}, m> to the replica nodes of the consensus group (⑤ in Figure 6);
iv. Receiving the pre-preparing message, the replica nodes of the consensus group performs verification operations. If the replica nodes of the consensus group accepts the pre-prepare message, it multicasts a <PREPARE, v, n, d, j > σ_j message to all other replica nodes of the consensus group; otherwise, the replica node j does nothing (⑥ in Figure 6);
v. The replica nodes of the consensus group accept preparing messages if the signatures are correct and their view number matches the current view v of the replica bodes. When a replica node of the consensus group receives prepare messages from $2f$ different replica nodes with high reputation values, p_1 broadcasts the message <EXIT, i, ip> to all nodes in the blockchain (⑦ in Figure 6);
vi. Nodes in the blockchain send a reply message <REPLY, v, t, j, r>, and remove the information of node i from the locally maintained NL table (⑧ in Figure 6);
vii. When node i receives $f + 1$ reply messages from different nodes, node i successfully exits the blockchain. Otherwise, node i will continue to perform tasks in the blockchain network.

2. Forced exit.
When the reputation value of node i is less than a special threshold for t consecutive rounds, the process of forced node exit from the blockchain is as follows:

(a) The preprocessing requests phase.
The primary node p_2 of consensus group detects that the reputation value of node i in the blockchain has remained below a specific threshold for t consecutive rounds. p_2 can directly issue a request <REQUEST, i, ip, pk, NL> to force node i to exit the blockchain;

(b) The consensus phase.
This phase aligns with the consensus stage of node voluntary exiting from the blockchain. Within the consensus group, nodes adaptively execute a three-stage or two-stage consensus based on the number of nodes with higher reputation value.

4. Performance Analysis of Cross-Institution Information-Sharing Network

In the context of cross-institution information-sharing networks based on consortium blockchains, our primary objective is to ensure the secure and efficient exchange of information among participating institutions. To achieve this, we employ cutting-edge technologies, specifically zk-SNARKs and proxy re-encryption, which serve to safeguard the integrity and privacy of the shared information. Additionally, to further enhance the efficiency of these cross-institution information-sharing networks, we introduce dynamic and adaptive PBFT consensus protocols.

This section is dedicated to providing a comprehensive analysis of the security and communication complexity intrinsic to our cross-institution information-sharing solution that is based on consortium blockchains.

4.1. Security Analysis

In the realm of blockchain technology, the utilization of a consortium blockchain in an inter-institutional information-sharing scheme provides a strong foundation for security. The immutability of data stored on the blockchain, coupled with the transparency and decentralization it offers, enhances the integrity and trustworthiness of the shared information.

Our cross-institution information-sharing scheme based on consortium blockchain utilizes advanced encryption technologies: zk-SNARKs and proxy re-encryption technology, significantly enhancing data confidentiality and privacy. Proxy re-encryption technology allows for secure data transmission and sharing between different institutions without the need for decryption and re-encryption at each step. The encryption technology ensures that even if data are compromised during sharing, it remains secure, thus ensuring security during information sharing. When combined with the inherent security features of blockchain, this multi-layer data encryption approach strengthens prevention against information leakage, network attacks, and internal threats, making it a viable solution for cross-institution information-sharing.

The introduction of a DA-PBFT consensus protocol in the context of a consortium blockchain serves as a pivotal means to ensure the efficiency and trustworthiness of cross-institution information-sharing networks. We employ a reputation mechanism to oversee the behavior of network nodes. This mechanism continuously evaluates their reputation based on their actions. When a node's reputation falls below a specified threshold, the consensus protocol can automatically expel the node from the blockchain network, thereby reducing the risks posed by malicious nodes to the integrity of cross-institution information-sharing. By enhancing consensus efficiency, we mitigate the risks of network congestion and latency, further fortifying the reliability of the information-sharing network.

In conclusion, we leverage blockchain technology, encryption techniques, and consensus protocols to establish a robust security foundation for cross-institution information-sharing networks based on consortium blockchain.

4.2. Communication Complexity Analysis

Communication complexity and message complexity are two important metrics used to measure the efficiency and performance of consensus protocols. Communication complexity $CommCplx$ quantifies the total number of information exchanges between nodes during the protocol execution. This includes the number of messages sent and received by each node. Message complexity $MsgCplx$ focuses on the total number of individual

messages exchanged between nodes in the consensus protocol; in this paper, we calculate communication complexity considering only the size of the messages $|\mathrm{m}|$.

The communication complexity $CommCplx$ for a new node joining/exiting the blockchain-based cross-institution information-sharing network is determined by the pre-processing communication complexity $CommCplx_{preprocessing}$ and consensus communication complexity $CommCplx_{consensus}$, as follows:

$$CommCplx = |\mathrm{m}|MsgCplx \tag{3}$$

$$CommCplx = CommCplx_{preprocessing} + CommCplx_{consensus} \tag{4}$$

To calculate the communication complexity of the pre-processing phase when a new node i joins the blockchain:

- In the JOIN-req phase, node i sends n messages;
- In the JOIN-pre phase, p_2 sends n_2 messages;
- In the JOIN-reply phase, n_2 observation group replica nodes send reply messages to p_2, then the communication times are n_2.

Therefore, the communication complexity of the pre-processing phase is as follows:

$$CommCplx_{preprocessing} = |\mathrm{m}|(n + 2n_2) \tag{5}$$

To calculate the communication complexity of the consensus phase when a new node i joins the blockchain:

- In the REQUEST phase, p_2 sends a request message to n_1 nodes in the consensus group, resulting in a communication time of n_1;
- In the PRE-PREPARE phase, p_1 sends a pre-prepare message to the consensus group's replica nodes, resulting in a communication time of n_1;
- In the PREPARE phase, n_1 consensus nodes multicast prepare messages, resulting in a communication time of n_1^2;
- In the JOIN phase, p_1 broadcasts a message to all nodes in the blockchain, resulting in a communication time of n;
- In the REPLY phase, all nodes in the blockchain reply to node i, resulting in a communication time of n.

Therefore, the communication complexity of the consensus phase when a new node joins the blockchain is as follows:

$$CommCplx_{consensus} = |\mathrm{m}|\left(2n_1 + n_1^2 + 2n\right) \tag{6}$$

Based on Equations (1)–(6) and Figure 5, the communication complexity of a new node i joining the blockchain is:

$$MsgCplx = \frac{1}{4}n^2 + 5n \tag{7}$$

$$CommCplx = |\mathrm{m}|\left(\frac{1}{4}n^2 + 5n\right) \tag{8}$$

The communication complexity of a node's exit from the blockchain consists of pre-processing communication complexity and consensus communication complexity, as shown in Equation (4). Therefore, the communication complexity of a node's exit from the blockchain is defined as follows:

$$CommCplx = |\mathrm{m}|\left(\frac{1}{4}n^2 + 5n\right) \tag{9}$$

We have analyzed the complexity of DA-PBFT on cross-institution information-sharing networks. As shown in Table 2 and Figure 7, the communication complexity of the DA-PBFT consensus protocol is compared with four other consensus protocols: PBFT [14], The Honey Badger of BFT Protocols [15], Hotstuff [16], and Foundation of Dynamic BFT [17]. Note that in Figure 7, we have calculated the percentages for The Honey Badger of BFT Protocols to make the data comparison more apparent. In blockchain systems, communication complexity is an important indicator to measure the efficiency and performance of consensus protocols. When the communication complexity is low, the efficiency of the consensus protocol improves, and the overall efficiency of the blockchain system increases.

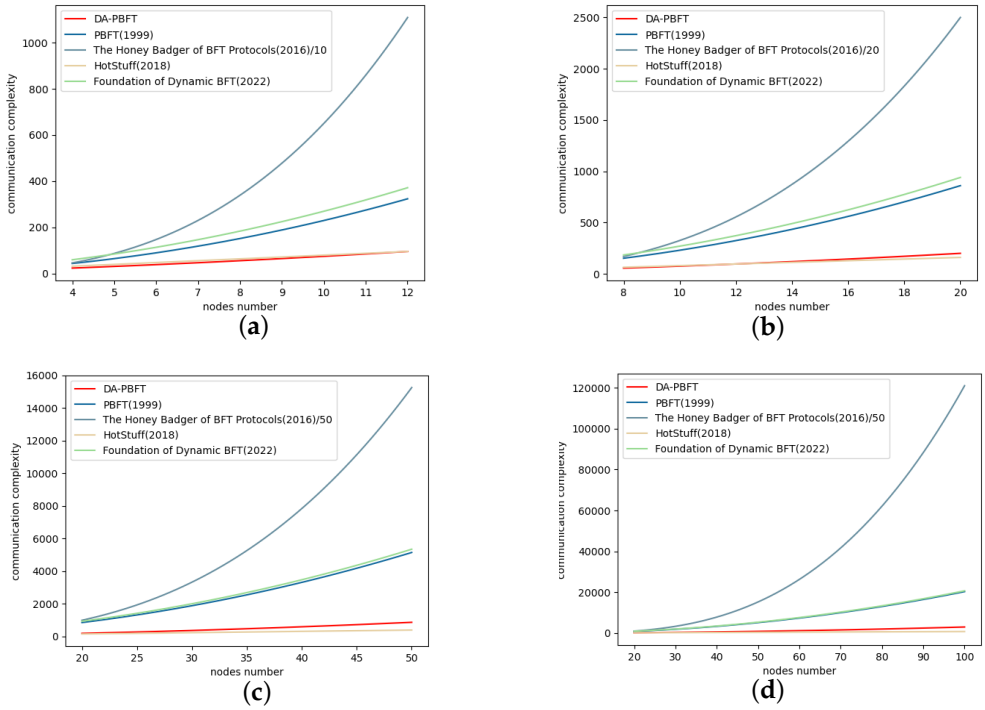

Figure 7. Comparison of communication complexity. (**a**) 4–12 nodes, comparison of communication complexity in DA-PBFT with other four consensus protocols ([14–17]). (**b**) 8–20 nodes, comparison of communication complexity in DA-PBFT with other four consensus protocols ([14–17]). (**c**) 20–50 nodes, comparison of communication complexity in DA-PBFT with other four consensus protocols ([14–17]). (**d**) 20–100 nodes, comparison of communication complexity in DA-PBFT with other four consensus protocols ([14–17]).

Table 2. The complexity comparison of the five algorithms.

	DA-PBFT	**PBFT (1999) [14]**	**The Honey Badger of BFT Protocols (2016) [15]**	**Hotstuff (2018) [16]**	**Foundation of Dynamic BFT (2022) [17]**
Deployment Scenario	Consortium blockchain	Consortium blockchain	Consortium blockchain	Consortium blockchain	–
Msg Cplx.	$\frac{1}{4}n^2 + 5n$	$2n^2 + 3n$	$6n^3 + 2n^2$	8n	$2n^2 + 7n$
Comm Cplx.	$\|m\|\left(\frac{1}{4}n^2 + 5n\right)$	$\|m\|(2n^2 + 3n)$	$\|m\|(6n^3 + 2n^2)$	$\|m\|(8n)$	$\|m\|(2n^2 + 7n)$
Fault Tolerant	$3f + 1 \leq n$	$3f + 1 \leq n$	$3f + 1 \leq n$	$3f + 1 \leq n$	$3f + 1 \leq n$

Note: the author derived the data through independent calculations based on pertinent references.

As shown in Figure 7a, when the blockchain network consists of 4 to 12 nodes, the communication complexity of our proposed DA-PBFT protocol is significantly lower than that of the other four consensus protocols. Figure 7b illustrates the comparison between DA-PBFT and the other four consensus protocols in a blockchain network with 8 to 20 nodes. In Figure 7c, the communication complexity of the five consensus protocols is compared

for a blockchain network with 20 to 50 nodes. Figure 7d demonstrates the comparison between DA-PBFT and the other four consensus protocols in a blockchain network with 20 to 100 nodes. From Figure 7, it is evident that the communication complexity of our proposed DA-PBFT consensus protocol is significantly lower than that of PBFT, The Honey Badger of BFT Protocols, and the Foundation of Dynamic. However, it is worth noting that when the number of nodes exceeds 12, the communication complexity of our proposed DA-PBFT protocol becomes slightly higher than that of the Hotstuff protocol. Nonetheless, it is crucial to consider that the Hotstuff protocol lacks support for dynamic addition or removal of nodes within the cross-institution information-sharing network, which is a key feature provided by our proposed DA-PBFT protocol.

In summary, in comparison to the work presented in Section 1, our research scheme extends the scope of information sharing to inter-institution collaboration. We have also employed consortium blockchain and cryptographic technologies to enhance trust and security among institutions during the process of information sharing. This stands in contrast to previous work that primarily focused on blockchain or consortium blockchains. Consequently, our solution offers heightened security. Furthermore, we have introduced the DA-PBFT consensus protocol specifically for cross-institution information-sharing networks. As illustrated in Figure 7, our proposed DA-PBFT significantly reduces network communication complexity, thereby improving consensus efficiency within cross-institution information-sharing networks. In conclusion, our proposed cross-institution information-sharing scheme based on consortium blockchain ultimately demonstrates favorable performance in promoting the security and efficiency of cross-institution information-sharing.

5. Conclusions

In summary, the proposed cross-institution information-sharing scheme based on consortium blockchain presented in this paper has contributed to the fields of blockchain consensus and its applications in inter-institutional information sharing, addressing the issues of privacy breaches and high communication complexity that exist in traditional cross-institution information-sharing. By combining on-chain transaction consensus with off-chain institutional storage and cryptographic techniques, the original information will not be exposed on the internet, and information cooperation and sharing among different institutions is secure. By introducing the DA-PBFT consensus protocol, faulted and malicious nodes are filtered out, and on-chain transaction consensus becomes secure and efficient significantly shown in the analysis results in Section 4. In other words, the proposed cross-institution information-sharing scheme based on consortium blockchain provides a solution to share information between two or more Institutions securely and effectively, and it can be applied in many fields, such as archives management for teachers and students in universities and schools, e-government information management, where lots of information related to personal privacy need to be shared. However, if it is applied in a system with frequent information sharing operations, the sharing efficiency will be limited by the limited storage and calculating resources. In conclusion, our work provides a direction for a safer and more efficient future for cross-institution information-sharing based on consortium blockchain.

Author Contributions: Conceptualization, B.T. and Y.C.; methodology, B.T. and Y.C.; software, B.T.; validation, B.T. and Y.C.; formal analysis, B.T., Y.C. and Y.Z.; investigation, B.T. and Y.C.; resources, B.T. and Y.C.; data curation, B.T. and Y.C.; writing—original draft preparation, B.T.; writing—review and editing, B.T., Y.C. and Y.Z.; supervision, Y.C., Y.Z., S.L. and Z.D. All authors have read and agreed to the published version of the manuscript.

Funding: This work is supported by the Science and Technology Major Project of Tibetan Autonomous Region of China under the grant No. XZ202201ZD0006G02, the Academic xinmiao Fund project of Guizhou Normal University under the grant No. Qianshixinmiao[2022]29, Guizhou Graduate Research Fund Project under the grant No. Qianjiaohe YJSKYJJ[2021] 104, and the Open Fund Project of Key Laboratory of Flight Technology and Flight Safety of CAAC (FZ2020KF10).

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/en/bitcoin-paper (accessed on 27 September 2023).
2. Chen, Z.; Zhu, Y. Personal archive service system using blockchain technology: Case study, promising and challenging. In Proceedings of the 2017 IEEE International Conference on AI & Mobile Services (AIMS), Honolulu, HI, USA, 25–30 June 2017; pp. 93–99.
3. Kamišalić, A.; Turkanović, M.; Mrdović, S.; Heričko, M. A preliminary review of blockchain-based solutions in higher education. In Proceedings of the Learning Technology for Education Challenges: 8th International Workshop, LTEC 2019, Zamora, Spain, 15–18 July 2019; pp. 114–124.
4. Lizcano, D.; Lara, J.A.; White, B.; Aljawarneh, S. Blockchain-based approach to create a model of trust in open and ubiquitous higher education. *J. Comput. High. Educ.* **2020**, *32*, 109–134. [CrossRef]
5. Leng, K.; Bi, Y.; Jing, L.; Fu, H.C.; Van Nieuwenhuyse, I. Research on agricultural supply chain system with double chain architecture based on blockchain technology. *Future Gener. Comput. Syst.* **2018**, *86*, 641–649. [CrossRef]
6. Saha, S.; Chattaraj, D.; Bera, B.; Kumar Das, A. Consortium blockchain-enabled access control mechanism in edge computing based generic Internet of Things environment. *Trans. Emerg. Telecommun. Technol.* **2021**, *32*, e3995. [CrossRef]
7. Merlec, M.M.; Islam, M.M.; Lee, Y.K.; In, H.P. A consortium blockchain-based secure and trusted electronic portfolio management scheme. *Sensors* **2022**, *22*, 1271. [CrossRef] [PubMed]
8. Kaur, P.; Parashar, A.; Duggal, K.; Sunita, S. A Blockchain-based Approach for Educators' Profile Management and Reward system. In Proceedings of the 2021 International Conference on Computing Sciences (ICCS), Phagwara, India, 4–5 December 2021; IEEE: Manhattan, NY, USA, 2021; pp. 206–211.
9. Liping, Q. Design of Archives Management Information System Based on Blockchain Technology. In Proceedings of the 2022 2nd International Signal Processing, Communications and Engineering Management Conference (ISPCEM), Montreal, QC, Canada, 25–27 November 2022; IEEE: Manhattan, NY, USA, 2022; pp. 66–72.
10. Yang, L.; Fang, S.; Sheng, L.; Dandan, L.; Hangxuan, S.; Yingying, W.; Nan, L.; Xin, C. Research and Application of Archive Data Management System Based on Blockchain. In Proceedings of the 2023 IEEE 2nd International Conference on Electrical Engineering, Big Data and Algorithms (EEBDA), Changchun, China, 24–26 February 2023; IEEE: Manhattan, NY, USA, 2023; pp. 1958–1962.
11. Zhao, Y.; Sun, J.; Long, Y.; Li, J.; Zhou, Z. Research on Model of Teacher Education Resource Sharing Platform Based on Consortium Blockchain. In Proceedings of the 2023 IEEE 6th Eurasian Conference on Educational Innovation (ECEI), Singapore, 3–5 February 2023; pp. 292–295.
12. Wu, G.; Wang, S.; Ning, Z.; Zhu, B. Privacy-Preserved Electronic Medical Record Exchanging and Sharing: A Blockchain-Based Smart Healthcare System. *IEEE J. Biomed. Health Inform.* **2022**, *26*, 1917–1927. [CrossRef] [PubMed]
13. Yu, S.; Huang, Y.; Tang, L.; Shen, B. Research on Information Sharing Mechanism Based on Blockchain Technology. In Proceedings of the 2022 7th International Conference on Computational Intelligence and Applications (ICCIA), Nanjing, China, 24–26 June 2022; pp. 210–214.
14. Castro, M.; Liskov, B. Practical Byzantine Fault Tolerance. In Proceedings of the Third Symposium on Operating Systems Design and Implementation, New Orleans, LA, USA, 22–25 February 1999; pp. 173–186.
15. Miller, A.; Xia, Y.; Croman, K.; Shi, E.; Song, D. The Honey Badger of BFT Protocols. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, New York, NY, USA, 24–28 October 2016; pp. 31–42.
16. Yin, M.; Malkhi, D.; Reiter, M.K.; Gueta, G.G.; Abraham, I. HotStuff: BFT Consensus with Linearity and Responsiveness. In Proceedings of the 2019 ACM Symposium on Principles of Distributed Computing, Toronto, ON, Canada, 29 July–2 August 2019; pp. 347–356.
17. Duan, S.; Zhang, H. Foundations of Dynamic BFT. In Proceedings of the 2022 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 23–25 May 2022; pp. 1317–1334.
18. Yurcik, W.; Woolam, C.; Hellings, G.; Khan, L. Measuring anonymization privacy/analysis tradeoffs inherent to sharing network data. In Proceedings of the NOMS 2008—2008 IEEE Network Operations and Management Symposium, Salvador, Brazil, 7–11 April 2008; pp. 991–994.
19. Goldwasser, S.; Micali, S.; Rackoff, C. The Knowledge Complexity of Interactive Proof-Systems. In *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*; Association for Computing Machinery: New York, NY, USA, 2019; pp. 203–225.
20. Blaze, M.; Bleumer, G.; Strauss, M. Divertible protocols and atomic proxy cryptography. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Espoo, Finland, 31 May–4 June 1998; Springer: Berlin/Heidelberg, Germany, 1998; pp. 127–144.

21. Kaur, S.; Chaturvedi, S.; Sharma, A.; Kar, J. A research survey on applications of consensus protocols in blockchain. *Secur. Commun. Netw.* **2021**, *2021*, 6693731. [CrossRef]
22. Lei, K.; Zhang, Q.; Xu, L.; Qi, Z. Reputation-Based Byzantine Fault-Tolerance for Consortium Blockchain. In Proceedings of the 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), Singapore, 11–13 December 2018; pp. 604–611.