Wireless Personal Communications (2022) 127:919–943
https://doi.org/10.1007/s11277-021-08451-x

A Hybrid Blockchain Model for Trusted Data of Supply Chain Finance

Jingkuang Liu[1] · Lemei Yan[1] · Dong Wang[1]

Accepted: 28 March 2021 / Published online: 8 April 2021

Abstract
Supply chain finance is an effective way to solve the problem of capital turnover of construction enterprises and stabilize economic growth under epidemic situation. Blockchain technology can solve the problems in the current supply chain finance business, such as incorrect information between banks and enterprises, lack of visibility in transaction process, and possible joint fraud in the core enterprise model. However, it still has problems such as inconvenient information verification, data fraud, and difficulty to achieve a balance between efficiency, security and cost. This paper presents a hybrid chain model combining PANDA (a consensus algorithm based on public chain) and X-Alliance (a consensus algorithm based on alliance chain). Such proposed hybrid chain model can process the transaction of each account in parallel, asynchronize from other unrelated accounts in the network, provide more reliable data storage and authority management, and ensure the ownership of change tracking data, which has higher performance and lower protection cost while ensuring data security and privacy security. According to the data of network crawling, the experimental results show that the throughput can reach 1200tps when four nodes are deployed. The model serves for the supply chain financial data management of engineering projects, making trade authenticity review, risk assessment and credit transmission of core enterprises more efficient. On this basis, each participant can carry out analysis and give early warning of capital flow, timely analyze and calculate the authenticity of transaction background. The proposed method provides a reference for the normal operation of the project fund under the COVID-19 epidemic.

Keywords Supply chain finance · Block chain · Hybrid chain data security

1 Introduction

From the end of 2019 to now, novel coronavirus has spread all over the world. Almost all projects under construction have encountered such difficulties as suspension of work, difficulty in financing the construction project and inhibited supply of production materials,

✉ Dong Wang
wangdong@gzhu.edu.cn

[1] School of Management, Guangzhou University, Guangzhou, Guangdong, People's Republic of China

etc., causing a huge impact on the current and future economic growth and normal fund operation of the project. According to the statistics of China Construction Industry Association, 90.55% of construction companies believe that the epidemic will cause construction delays; 55.85% believe that the epidemic situation will prevent the project from being delivered as scheduled; and 42.41% of enterprises point out that the upstream supply chain such as raw materials has been disrupted. The shutdown caused by the epidemic increased the operating costs and construction expenses of construction enterprises, and 68.91% of construction enterprises experienced double pressure in capital turnover and cost management and control [1]. In essence, the epidemic has brought great challenges to construction enterprises in terms of cash flow control, risk management and control, information coordination, and some enterprises are facing difficulties in capital turnover.

Supply chain finance is a key way to ensure the normal capital turnover and stable economic growth of construction enterprises. It is possible to realize accurate control and mutual benefit and win–win results between banks and enterprises using digital approaches under the epidemic situation. Banks can stand at the height of the whole industry, integrate the production factors such as scattered information, data and capacity, and make financing arrangements for all member enterprises, carry out whole-process tracking management, real-time dynamic analysis and risk prevention and control, information sharing among members, and collaborative operation of engineering projects, so as to improve the capability of financing services, logistics services, and financial services, which guarantees the continuity of capital chain to the greatest extent in the case of sudden impact. Previous report has pointed out that promoting the construction of industrial supply chain platform and establishment of centralized procurement and financial service platform of construction industry is a new direction related to the application of supply chain finance in the construction industry. Affected by the epidemic, joint fraud may occur in the current supply chain finance business due to the information asymmetry between banks and enterprises [2–5] and the lack of visibility of the whole transaction process [3, 6, 7], In this case, banks or other capital ends will not only worry about the repayment ability of the enterprise but also care about the authenticity of the transaction information itself. They will invest a lot of human, material and financial resources to verify the authenticity of the transaction, but little effect can be achieved. In response to these problems, Tung et al. found that blockchain technology could effectively solve problems in data trust, data exchanging, data transmission and analysis [8, 9].

Block chain technology enables supply chain finance to solve engineering construction enterprises' pain points in financing. Intelligent supply chain financial service platform based on block chain technology provides real-time and reliable view of transaction status for supply chain finance, effectively improves transaction transparency, ensures data security, and fully prevents risks in the whole cycle of data collection [10], storage, transmission, sharing and destruction. This technology platform can manage and deal with all kinds of hidden dangers brought by data processing. By establishing trust mechanism, it can bring better capital liquidity, improve the stickability of upstream and downstream enterprises to core enterprises, and further enhance the competitiveness of core enterprises in the same industry, thus solving the financing problem of engineering construction enterprises.

A reliable and stable financial service platform needs an efficient and advanced system architecture to solve the network congestion, high transaction costs, and slow transaction processing speed caused by increased business volume. In addition, due to the high network latency in point-to-point network, the order of transactions observed at each node cannot be completely consistent. Therefore, there is a need to design a mechanism for

blockchain systems to reach an agreement on the sequence of transactions occurring at about the same time. This algorithm of reaching consensus on the sequence of transactions within a time window is called a "consensus mechanism", which is mainly used to improve the overall performance of the supply chain finance platform. As one of the core technologies of blockchain, consensus algorithm directly affects the security and trust of blockchain [11]. In a blockchain, each transaction is verified for consistency within a decentralized system and stored in a block format [12]. Reaching consensus among all the participants in the network is a key feature of blockchain technology before permanently recorded [13, 14]. The participants in the network then proceed to validate the information and create a block. Each block is connected to another block of the chain [15, 16], so as to provide traceable and transparent information to all members. This paper intends to design a new consensus algorithm for supply chain finance of engineering projects, which can provide more reliable data storage and access management, ensure the tracking data ownership, so as to solve the problems in information sharing and collaborative operations between members, improve the efficiency of project follow-up management, dynamic analysis and risk prevention and control, thus providing the basis for business decisions.

The rest of this article is arranged as follows. The second section introduces the blockchain concept, consensus algorithm and other core technologies. The third section introduces the optimization idea and process of the improved hybrid chain model. The fourth part simulates the hybrid chain model and analyzes the experimental results. Finally, the thesis is summarized and the future development direction is prospected.

2 Literature Review

Blockchain technology is basically a distributed database of public/private ledgers that record or share all digital events that have been executed and shared among participating blockchain agents [11, 17], The history of blockchain technology can be traced back to distributed ledger technology. Blockchain technology differs from most existing information system designs in that it includes four key features: decentralization, non-tampering, traceability and intelligent contracts.

Consensus algorithm is the most important factor in the whole blockchain system, and its efficiency directly determines the performance of blockchain. With the continuous development of blockchain technology, consensus algorithm has experienced emerging demands from the earliest Proof-of-Work (PoW) [17, 18] to later Proof of Stake (PoS) [19] and Delegated Proof of Stake (DPoS) [20]. Meanwhile, the consensus algorithm has undergone the evolution from Practical Byzantine Fault Tolerance (PBFT) [21] to some other improved consensus algorithms, such as Proof-of-Burn (PoB) [21], Proof-of-Luck (PoL) [22] and Stellar Consistency Protocol (SCP) [23]. However, there is still no perfect consensus algorithm that can effectively solve the relationship between the increase of node number and the rapid increase of time–space complexity.

Proof-of-Work (PoW) mechanism is the first consensus protocol of blockchain. Bitcoin adopts PoW protocol to reach consensus, of which the core idea is to introduce the computing power of distributed nodes to compete and ensure the consistency of data and security of consensus. The PoW consensus algorithm requires all nodes in the system to solve a computationally complex but easily verified mathematical problem based on their own computing power. The node that solves the problem the fastest will get the right to package a block. Therefore, PoW protocol has some problems: (1) PoW

process usually consumes a lot of computing resources and energy; (2) PoW has serious efficiency problems, because the generation of each block takes time and the newly generated block needs the confirmation of subsequent blocks to ensure its validity, which takes longer time; (3) The security of PoW protocol requires that the computing resources occupied by an attacker is no more than 50% of the computing resources of the entire network.

To reduce the waste of computing resources in the PoW, PoS takes advantage of the stakes in competition to obtain the opportunity to generate blocks [24]. However, when a node holds a large amount of equities for a long time, the probability of calculating nonce value is close to 100%. Although the time to generate blocks is reduced to only 64 s [24], PoS still relies on computing power and wastes a lot of computing resources. To break the competitive cycle of generating blocks for computing resources, DPoS introduces a PoS-based voting mechanism which reduces the time cost of generating blocks to 3 s [25]. PoS classifies the nodes in the blockchain system into three categories: witness node, delegate node and work node. Witnesses are voted through the resources of all nodes, which is the core of the system. The N nodes with the most votes become witness nodes and generate blocks in turn. Although not paid, the representative can initiate a request to update the blockchain. Employees have the right to propose new projects and receive incentives from elected projects. However, in the course of the negotiation, witnesses will not be disqualified except for special reasons, they will become witnesses and have the right to generate blocks for a long time, which leads to the security risk caused by the high concentration of DPoS. In addition, malicious nodes can exist in any blockchain. The so-called malicious nodes refer to the nodes that illegally violate the trusted consensus mechanism, tamper with trading information, cause network congestion and disrupt the normal operation of the network [26]. As a result, blockchain systems can become insecure, unreliable and inefficient.

In recent years, academia has paid intensive attention to the research on blockchain security and privacy threats. Ouaguid et al. [27] proposes a new framework based on blockchain technology, which allows to extract and analyze the requested permissions in an Android application via a decentralized and distributed system. Kaushik et al. [28] uses a hierarchical identity-based encryption to protect data security and check data integrity to ensure that malicious attackers or CSPs will not change or modify for their own benefit. Sumathi et al. [29] ensures better security and integrity of user sensitive attribute values. Using the distributed storage system, the account holder information is divided into sensitive and non-sensitive attributes. Esposito et al. [30] proposes a novel solution for distributed management of identity and authorization policies by leveraging on the blockchain technology to hold a global view of the security policies within the system, and integrating it in the FIWARE platform. To ensure the robustness and security of digital image watermarking, Li et al. [31] propose a novel algorithm using synergetic neural networks. Nedjah et al. [32] propose an effective implement of fingerprint verification on smart cards, which is based on the Skin Elastic Tolerance Algorithm (SETA). It uses minutiae to implement fingerprints matching, guaranteeing the maximum security and privacy. Research on the security and privacy of blockchain mainly focuses on two aspects: (1) adopt distributed management to protect data security, and (2) specific suggestions for data security in different scenarios.

In general, there are still deficiencies such as inconvenient information verification, falsification of data, and difficulty in achieving a balance among consensus efficiency, security and cost. The improved consensus algorithm proposed in this work integrates PoW with the idea of fairness and DPoS with the idea of reducing resource consumption and

improving consensus efficiency of block chain system, which not only guarantees data security and privacy security, but also has higher performance and lower protection cost.

3 Trusted Data Hybrid Chain Model

3.1 Symbol

The main symbols involved in this paper and their definitions are shown in Table 1.

3.2 Hybrid Chain Model Structure

At present, there are mainly two kinds of data protection schemes based on block chain, where one scheme realizes data protection by only using alliance chain, and the other realizes data protection by only using public chain. The former reduces the cost of data protection and has high consensus efficiency and high transaction throughput due to controllable alliance nodes. The latter has higher security, but at the same time has higher data protection cost. For sensitive data, the owner does not want the data to be stored in an open database even if it is encrypted, because encrypted data exposed to the public not only increases the risk of data leakage, but also increases the possibility of data attack. This paper proposes a trusted data hybrid chain model for supply chain finance, called DFB for short. This model is composed of both license chain and non-license chain, which has high performance and low protection cost while ensuring data security and privacy security. The overall structure of proposed hybrid model is shown in Fig. 1.

This paper proposes a new consensus algorithm based on common chain, which is a hybrid chain model combining alliance and x-alliance. The model has a double DAG structure, that is, each account has its own account DAG structure, and all accounts constitute the entire account DAG. Each account consists of a data tree and a key certificate, which is divided into NorCA and ConCA. The NorCA includes four processes: TBcreate, TBsend, TBreceive and TBdeal.

3.2.1 Consensus Node

A consensus node is actually a piece of software running on a computer, which follows the model protocol and participates in the model network. The nodes communicate with each other through a P2P network formed by the Gossip protocol. Each consensus node holds the same book, recording the securities assets and data assets, respectively. In addition, each ConNode initializes and creates a unique CAccount corresponding to it. The created CAccount is composed of public–private key pair $<$Pub, PriK$>$, in which the public key Pub is called the account address and is used to identify the ConNode and make it publicly available. The CAccount needs to lock the consensus margin before reaching consensus, which gives the CAccount the right to receive bifurcateed fines and the risk of forfeiture of the consensus margin.

3.2.2 Account

The account is the entity that the actual user participates in the system. The account is composed of public and private key pair <Pub, PriK>, in which the public key Pub

Table 1 Symbols involved in this paper and their definitions

Symbol	Definition
<Pub, PriK>	Public key, private key
ConNode	Consensus nodes in a hybrid chain
CAccount	Account in the hybrid chain
NorCA, ConCA	Common account and consensus account in the hybrid chain
DataAuthen	Data authentication in the hybrid chain
TBcreate, TBdelegate, TBreceive, TBdeal, TBauth	transaction create block, transaction delegate block, transaction receive block, transaction deal block and transaction authentication block
State(Stb) = {Ssending, Spending, Sreceived}	The transaction block Stb state consists of Ssending state, Spending sate and Sreceived state
F	Safety parameter
<Pub-mem, PriK-mem>	Member public keys and member private keys in the alliance chain
MemSign	Member signatures in the alliance chain
AttackNo	The number of malicious nodes in the alliance chain
Loyalt	The percentage of loyal users in the alliance chain who hold key licenses
XALT	Key license in alliance chain
Com-total, Com-ActNode, Com-ExpCo	The size of the steering committee in the public chain, the actual number of nodes, and the expected number of consensus identities
Committee	Steering committee
Candidate-Seed	The candidate consensus node of the same former block hash Seed
Committee-Seed	the consensus committee for hash Seed bifurcate of the same former block
State(Stb-Consensus) < = {Panda-vote, Panda-commit}	The consensus phase in the PANDA consensus
State(Message-type) < = {Message-vote, Message -commit}	Consensus message type in the PANDA consensus
ComID-seed, ComID-cons	Consensus identity in the PANDA consensus and consensus identity in DPoS-Quorum
ID-good	Threshold of honest identity
Max-vote	The maximum time of the voting period
Max-term	The maximum term of consensus
h(x)	Hash function with a number as output
H(x)	The hash function, the output is the point on the curve

is used to identify the account and make it publicly available on the web. A user can control multiple accounts, but each account can only correspond to one public key. The private key PriK is similar to the password in the ordinary system. The user holding the private key has the actual control of the account, and can use the private key PriK to sign the trading block or message, so as to determine the source of the trading block or message. The account is divided into the normal account (NorCA) and the

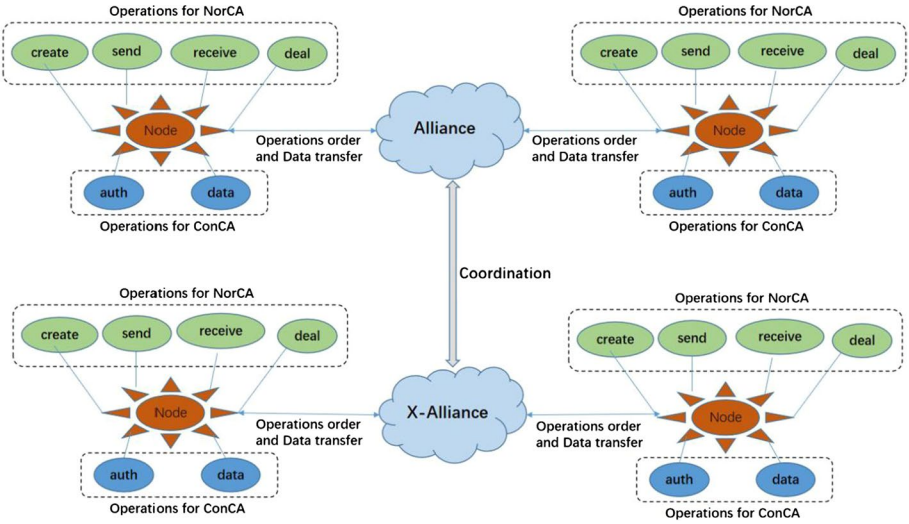

Fig. 1 Structure of hybrid chain model

consensus account (ConCA). NorCA owns the card ledger and the data ledger, which can be used to send and receive card assets and data assets, and distribute access and control rights of the data assets. A ConCA has the same functions as a NorCA in addition to the functions described in the definition of the consensus node. Each Account has its own Account DAG structure, which is called Account-DAG. The whole model structure composed of all Account-DAG is called Node-DAG.

3.2.3 Transaction Block

A transaction is an agreement or action between the receiver and receiver. In the hybrid chain model, the construction of a transaction block requires the account owner to sign with a private key, and one block contains only one transaction, so it is called a Transaction Block and recorded as TB. The transction block is divided into transaction create block (TBcreate), transaction delegate block (TBdelegate), transaction receive block (TBreceive), transaction deal block (TBdeal) and transaction authentication block (TBauth). Asset transfer requires the joint confirmation of two transaction blocks. Transaction block is divided into three states (Stb) = {Ssending, Spending, Sreceived}, which means sending State-Ssending, spending State-Spending, receiving State-Srecelved. In one transaction, the sending account builds and broadcasts the transaction TBsend, and this block state is Ssending state and then changes into Spending state after all nodes receive it (consensus completed). When the receiving account is logged, it will receive assets according to the transaction TBsend and constructs the corresponding received transaction TBreceived or dealed transaction TBdeal. At this time, the block state changes into Sreceived and a transaction is completed.

3.3 Consensus Algorithm Based on Hybrid Chain Model

Consensus algorithm is mainly used to determine distributed ledger among nodes in blockchain according to a pre-agreed rule, making different nodes reach consensus on transaction data, so as to ensure the consistency and authenticity of distributed ledger. Its essence is that different nodes adopt distributed consensus mechanism to reach consensus on the structure of blockchain.

The PoW consensus algorithm used in Bitcoin is prone to resource waste, requires a long transaction confirmation time, and has a low transaction throughput. The Proof of Stake (PoS) algorithm uses the weight held by the block chain accounts to replace the hashrate in the PoW algorithm, and solves the problem of resource consumption. However, it is limited by some deficiencies such as "Nothing at Stake" and" long distance attack ". For example, the DPoS algorithm used in blockchain projects such as EOS achieves consensus through selected agents, which shows centralized features to a certain extent and has the possibility of suffering from DDoS attack or collusion between nodes. For the improved traditional distributed consistent consensus algorithm, such as PBFT, the message propagation complexity in the algorithm increases exponentially with the increase of the number of consensus nodes, so it is more suitable for the application scenario of alliance chain.

This paper designs PANDA (a consensus algorithm suitable for public chain environment) and DPoS-Quorum (a consensus algorithm suitable for federated chain environment) to help nodes in block chain reach effective consensus. Moreover, the formula algorithm of the proposed hybrid chain model is obtained according to PANDA consensus-based public chain Alliance and DPoS-Quorum consensus -based alliance chain X-Alliance.

3.3.1 Alliance Chain

Alliance chain, also known as license chain, is composed of organizations, institutions and individuals with a common goal. The consensus of the alliance chain involves the participation of all alliance members, the read–write access permission of data is formulated according to the rules of the alliance, and the joining of member nodes should be reviewed by other nodes of the alliance. In the hybrid chain model, the alliance chain is mainly responsible for storing the original data and recording the storage information and data attribute information. The alliance chain in the model can adopt either the mainstream alliance chain based on Ethereum model or the alliance chain based on super ledger. In this paper, a DPoS-Quorum consensus-based alliance chain algorithm X-Alliance is designed for the alliance chain environment, where X represents the specific application scenario.

(1) Hypotheses

Hypothesis 1: The honest nodes in the alliance chain run the safe and reliable model software, and the proportion of the number of key certificates held by the honest users is greater than the threshold Loyalt, while the malicious nodes can join the alliance chain and have a certain number of key certificates;

Hypothesis 2: There are at least 2AttackNo + 1 honest nodes in the alliance chain, and the total number of nodes in the public chain is at least $3AttackNo + 1$.

Hypothesis 3: Messages sent by honest users in the alliance chain can be received by other honest users within a certain time Max-term, and network partitioning is not allowed.

Hypothesis 4: If the probability is small, it means that the probability of its occurrence is at most $O\left(\frac{1}{2}\right)^f$, where f is the safety parameter. Similarly, if the probability of occur-

rence of an event is high, the probability of the occurrence of such event is at least $1 - O\left(\frac{1}{2}\right)^f$.

(2) Alliance chain algorithm X-alliance based on DPoS-Quorum consensus.

In the X-Alliance chain, when a new consensus account is created, or consensus bifurcate or even storage mistrust occur, the DPoS-Quorum consensus-based alliance chain algorithm x-Alliance can be used to help the nodes in the alliance chain reach an effective consensus. In the process of consensus, the alliance chain no first determines whether it has a legitimate identity to participate in the consensus committee to solve the proposal through verifiable random function (VRF). If it has a legitimate consensus identity, it can participate in and vote on the consensus. When the number of collected votes for a certain proposal exceeds the legal threshold, the consensus is reached and the entire consensus process ends.

Step 1: Setting up

When a new node ConNode_iin the alliance chain joins the existing consensus node, the member public key needs to be updated, denoted as Pub-mem-new = h1*Pub-mem1 + h2* Pub-mem2 + … + hn* Pub-memn, where hi = h(Pub-mem1|| Pub-mem2||…Pub-memn). At this point, the member signature is updated to MemSigni = (hi*PriK-memi)*H(Pub-mem-new, i). When the consensus nodes in the alliance chain receive the new node's public information <Pub-memi, MemSigni>, each consensus node needs to update its Pub-mem-new and its member private key PriK-mem locally. The private key of the new node is recorded as Prik-memi, where.

PriK-memi = (h1*PriK-mem1)*H(Pub-mem-new,i) + (h2*PriK-mem2)*H(Pub-mem-new, i) + … + (hn*PriK-memn)*H(Pub-mem-new, i).

Step 2: Consensus

① Proposes

The proposes in the consensus procedures can be classified to the following types:

The first type: propose to create a new consensus account to verify whether the existing consensus nodes in the alliance chain allow the new consensus account to be added to the alliance chain, denoted as CAccount_create.

The second type: propose to anchor the data into the public chain to express the anchor information of each account, which is denoted as CAccount_anchor.

The third type: propose to reach a consensus on a bifurcate, that is, propose to select a certain transaction block TB to reach consensus for transaction blocks with the same pre-block hash, which is denoted as CAccount_bifurcate;

The fourth type: proposes to store nodes or accounts that do not trust each other, which means the storage margin may be deducted through this proposal if the node storing the data is found not to provide a valid data acquisition service, or is unwilling to pay the data storage fee, denoted as CAccount_storage.

② The generation of consensus identity

When a consensus node in the alliance chain receives the proposal, it can determine whether it has a legitimate consensus identity to participate in the proposed consensus committee by calculation of its equity using VRF. If it has a legitimate consensus status, then it can vote for consensus. The consensus identity generation algorithm selects the corresponding consensus identity based on the weight held by the node and calculates its voting weight. The consensus identity generation algorithm is shown in Fig. 2. If the calculated value of consensus identity voting weight is 0, the identity is illegal. The legitimate consensus identities form a consensus committee to resolve the proposal.

Algorithm 1: To generate legitimate consensus identities ConsensusIDGeneration()

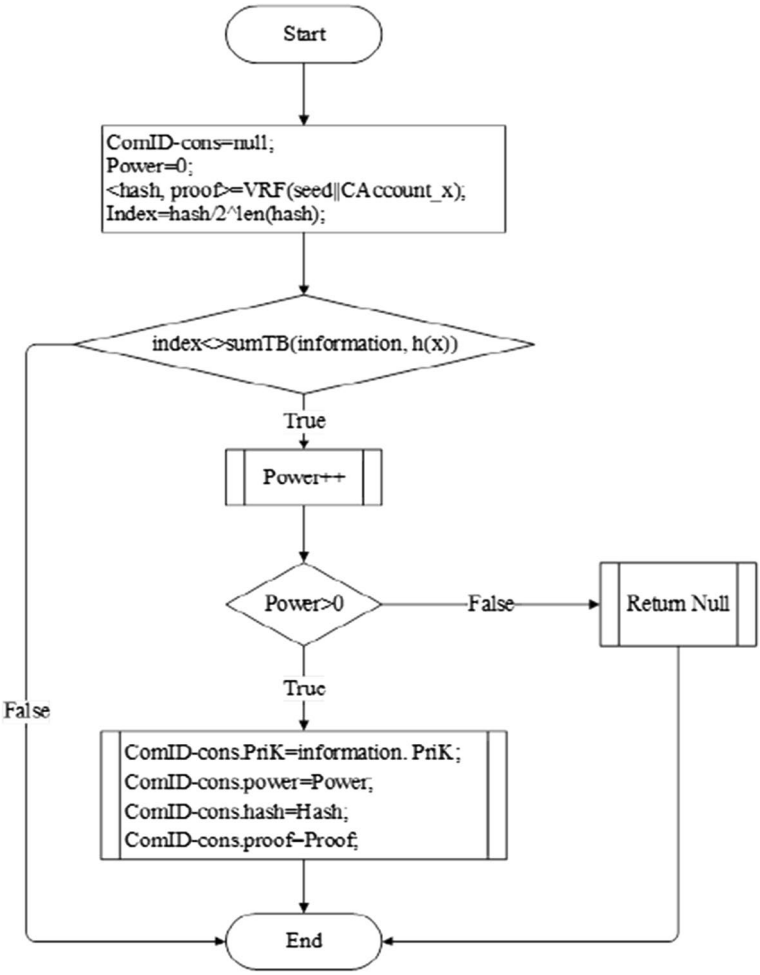

Fig. 2 Generation process of alliance chain consensus identity

Input: w-node's weight; information-context information of node; seed-the pre-block hash; CAccount_x-proposal type

③ Voting

Consensus nodes with legal status vote for consensus according to accepted proposals, which is denoted as MemSigni = PriK-mem*H(Pub-mem-new, CAccount_x) + PriK-memi. The consensus identity and proposed hash value of this node transmit information to other nodes in the alliance chain.

④ Vote counting

The nodes in the alliance chain count the number of consensus votes received. When the number of votes for a certain proposal exceeds the legal threshold and the signature collection passes the authentification, the consensus nodes reach consensus on the proposal. The legal threshold depends on the security parameter f.

Compared with the traditional blockchain system, which needs to verify the signature of each consensus vote, the alliance chain designs a way to verify the

signature through collection of signatures, that is, to collect the signatures as a package (where the number of signatures exceeds the threshold) for signature verification at one time, which improves the efficiency of the signature verification. SignCollection can be represented as SignCollection = MemSign1 + MemSign2 + … + MemSigni. The corresponding public key collection for SignCollection is denotable as Pub-SignCollection = Pub-mem1 + Pub-mem2 + … + Pub-memi.

Proposition 1: if stage(Pub-SignCollection, SignCollection) = stage(Pub-SignCollection, H(Pub-mem-new, CAccount_x)*stage(PriK-mem, H(PriK-mem1, 1) + H(PriK -mem2, 2) + … + H(PriK -memi,i))), the nodes in the alliance chain reach consensus on CAccount_x.

Prove:
Stage (Pub-SignCollection, SignCollection)
=Stage(Pub-SignCollection, MemSign1 + MemSign2 + … + MemSigni)
=stage(Pub-SignCollection, PriK-mem*H(Pub-mem-new, CAccount_x) + PriK-memi)
=stage(Pub-SignCollection,PriK-mem*H(Pub-mem-new,CAccount_x)*stage(Pub-SignCollection, PriK-memi)
=Stage(Pub-SignCollection,H(Pub-SignCollection,CAccount_x))*stage(Pub-SignCollection, (h1*PriK-mem1)*H(Pub-mem-new,i) + (h2*PriK-mem2)*H(Pub-mem-new,i) + … + (hn*PriK-memn)*H(Pub-mem-new, i)).

3.3.2 Public Chain

Public chain is also called non-licensed chain. Any organization or individual is free to join or quit the blockchain system, and all members of the system can participate in consensus and have access to read and write data. In the hybrid chain model, the public chain anchors the block snapshot information of the license chain to further protect the security of the license chain. Moreover, the public chain can package and anchor multiple block snapshots of the license chain, thereby saving protection costs. The public chain in the model can be the current mainstream bitcoin or Ethereum public chain. The PANDA consensus-based Alliance chain algorithm (Alliance) which is suitable for public chain environments is designed in this paper.

(1) Hypotheses

Hypothesis 1: The honest nodes in the public chain run the safe and reliable model software, and the proportion of the number of key licenses held by the honest user is greater than the threshold Loyalt, while the malicious node can join the non-license chain and have a certain number of key licenses.

Hypothesis 2: The strong synchronization hypothesis, that is, information sent by honest users in the public chain can be received by other honest users in the non-licensed chain within a certain time Max-vote, and network partitioning is not allowed.

Hypothesis 3: The weak synchronization hypothesis, that is, the public chain may have a long but certain asynchronous time period, after which there must be a reasonable and long strong synchronous time period.

Hypothesis 4: If the probability is small, it means that the probability of its occurrence is at most $O\left(\frac{1}{2}\right)^f$, where f is the safety parameter. Similarly, if the probability of occurrence of an event is high, the probability of the occurrence of such event is at least $1 - O\left(\frac{1}{2}\right)^f$.

(2) Alliance-alliance chain algorithm based on PANDA consensus.

Step 1: Bifurcate observation

The transaction block can only be constructed by the sending account rather than by a third party. This means that an evildoing account can only attempt to cause a bifurcate by constructing multiple sending transaction blocks with the same pre-block hash value on its key license chain. A transaction block bifurcate occurs when two (or more) transaction blocks contain the same pre-block hash value.

Assume that CAccount-send also constructs multiple transaction blocks with the same H(Pre) value, which are recorded as $\text{List}_{\text{TB}} = \{\text{TB1\_send, TB2\_send, TB3\_send, } \ldots\ldots\}$ broadcasted to the model. The nodes in the model will observe the bifurcation transaction collection {TB1_send, TB2_send, TB3_send, ……}, thus forming a bifurcate. Since the key authorization chain is a one-way sequential chain, the consensus algorithm is needed to help the consensus nodes select a certain transaction block from the bifurcated collection List_TB and add it to its Account-DAG.

If no bifurcate is observed by consensus nodes, the transaction block is directly added to its Account-DAG; If the consensus nodes observe the occurrence of bifurcation (at this point, such consensus nodes are called Candidate consensus nodes referred to as Candidate-seed, where seed represents the same pre-block hash H(Pre) in the bifurcation transaction block, which is denoted as seed ← H(pre). Because of the existence of bifurcation penalty incentive, the Candidate-Seed will actively participate in the consensus in order to obtain bifurcation penalty.

Step 2: Generation of consensus identity

When the nodes in the model observe a bifurcate, the candidate consensus node begins to calculate the legitimate consensus identity and wish to participate in the consensus to resolve such bifurcation. Each Candidate-Seed has a unique consensus identity at each stage of the consensus, denoted as ComID-seed ← <Stb, Panda-vote, Panda-commit>. The candidate-Seed in the model computes the hash value $h(x) \leq w_i/W$ that meets the PoS condition secretly and locally, and forms a legal consensus identity to participate in the consensus together with its public key and other information, denoted as ComID-cons ← <h(x), proof, message>, ComID-seed ← <Stb, ComID-cons, Panda-vote, Panda-commit>.

Each candidate consensus node calculates multiple legal identities for consensus based on its voting weight secretly and locally. w_i is the sum of the voting weights held and represented by the node (hereinafter referred to as the node weight); W represents the total voting weight in the model. These parameters joint determine the difficulty in calculating consensus identity. The greater the weight held by the node, the more consensus identities will be generated under the same number of calculation attempts, and the greater the probability of obtaining the bifurcation penalty.

Step 3: Formation of consensus committee

When the candidate consensus node computes the consensus identity secretly and locally, the consensus committee to resolve the bifurcation is also generated in the meantime, which is denoted as Committee-Seed. In the first stage of public chain information transmission, each candidate consensus node corresponds to a unique consensus identity and joins the consensus committee. In the next stage, the candidate consensus node secretly and locally calculates multiple consensus identities according to its weight, uses VRF to calculate the hash value secretly and locally, and then calculates the consensus identity satisfying the PoS condition based on such hash value. The public key Pub, private key PriK, account weight W1, model total weight W and configuration information of each consensus account are collectively referred to as the context information of the consensus node, denoted as information, as shown in Fig. 3.

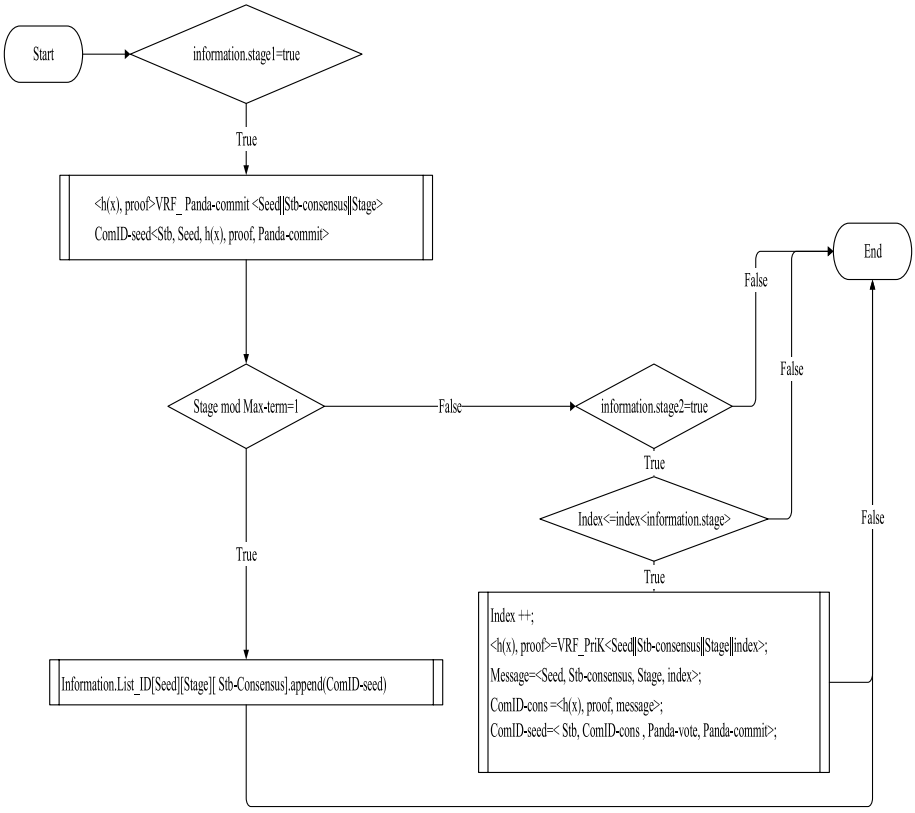

Fig. 3 Production process of public chain consensus identity

Algorithm 2: The generation of consensus identity

Input: Information-the node's context information; Seed-The pre-block hash; Stb-Consensus—the Consensus stage; Stage—Current term

To verify that consensus identity whether ComID-seed is a legitimate member of the Consensus Committee Committee-Seed, a process is designed as shown in Fig. 4.

Algorithm 3: Verify that whether the consensus identity belongs to the corresponding consensus committee

Input: ComID-seed-Consensus identity; Stb-consensus- Consensus stage

Step 4: Consensus stage

While the consensus committee coming into being, the consensus emerges. Consensus is divided into two stages, denoted as State (Stb-Consensus) < = {Panda-vote, Panda-commit}. In the consensus stage Panda-vote, the members of the consensus committee choose a trading block to vote, and all consensus nodes in the model collect the vote results of the consensus committee. In the consensus stage Panda-commit, the members of the consensus committee make a commit vote according to the collected vote, and all the consensus nodes in the model collect the commit vote results of the consensus committee. When the commit vote results exceed the voting threshold ID-good, the vote ends. The core process of consensus is shown in Fig. 5.

Algorithm 4: The core process of consensus PANDA_Consensus()

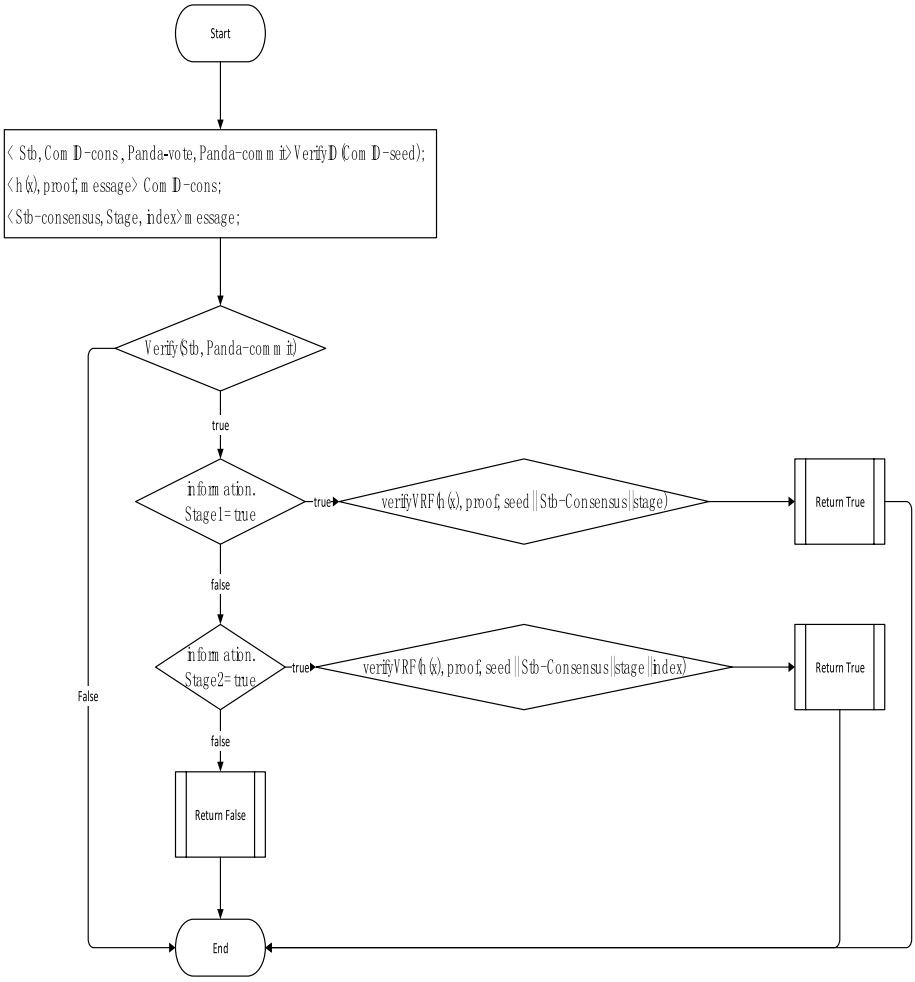

Fig. 4 Flow chart of public identity verification

Input: Information-the node's context information; Seed—The pre-block hash
Stage ← 1; H(select-TB) ← null; H(TB) ← null; List_TB ← null.

3.4 Algorithm Analysis

3.4.1 Safety

The Committee Act represents the actual size of the consensus Committee. Num_Honest represents the number of honest identities that have been committed to transaction block during the stage term, and $1 <= \text{Num\_Honest} <= \text{ID-good}$. In the stage + 1 consensus stage, Num_Honest will continue to vote. Num_Fake represents the number of malicious identities who can vote, reject, or abstain, $\text{Num\_Fake} <= \text{ID-good}$. Num-Rest represents the number of remaining identities, $\text{Num\_Honest} + \text{Num\_Fake} + \text{Num-Rest} = \text{Committee\_Act}$.

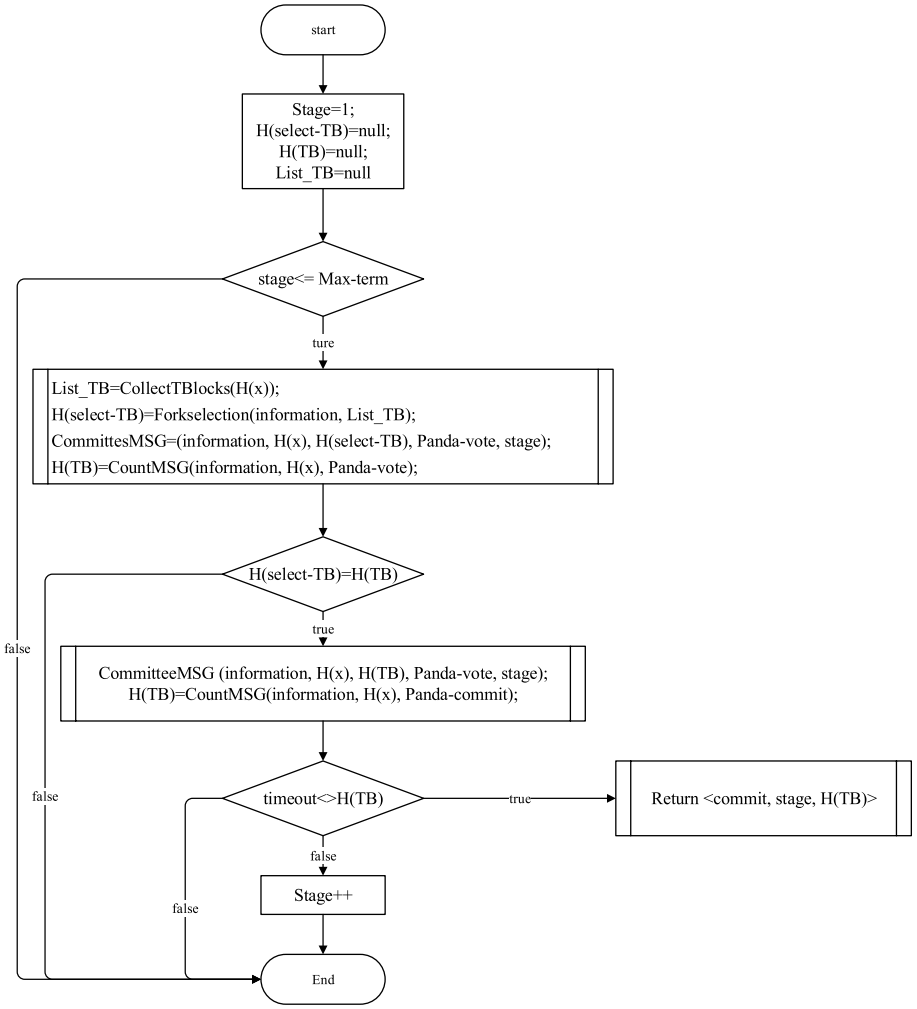

Fig. 5 Flow chart of consensus process

Num-Rest0 represents the number of remaining identities who vote during the consensus stage, then the difference between Num-Rest and Num-Rest0 represents the number of identities who have not voted. When a consensus identity commits a transaction block late, the remaining Num_Fake + Num-Rest identities do not reach consensus on the current transaction block, that is, Num_Fake + Num-Rest- Num-Rest0 < ID-good.

Proof:(proof by contradiction)
Suppose Num_Fake + Num-Rest- Num-Rest0 > = ID-good,
Num_Fake + Num-Rest- Num-Rest0 + Num_Honest > = ID-good + Num_Honest
Committee_Act- Num-Rest0 > = ID-good + Num_Honest
Num_Honest + Num-Rest0 < = Committee_Act- ID-good
Considering the aforementioned algorithm hypothesis 1, Committee_Act = Num_Fake + ID-good < 3* ID-good/2

Num_Honest + Num-Rest0 < ID-good/2

When all malicious nodes vote on the current transaction block, that is Num_Honest + Num_Fake + Num-Rest0 > ID-good. At this time, Num_Fake < ID-good/2, Num_Honest + Num-Rest0 > ID-good/2 contradicts the hypothesis. So the hypothesis is not true. In the process of consensus, the nodes in the model can only reach consensus on a certain sending transaction block in the bifurcate collection, but not on other transaction blocks in the bifurcate collection.

3.4.2 Analysis of Vector of Attack

Witch attack. If there is no trusted public key infrastructure in the model, the malicious node can simulate multiple virtual nodes to create a large number of useless witch nodes. A malicious node can create hundreds of witch nodes. In this paper, whether the PANDA consensus or the DPoS-Quorum consensus, the identity participating in the consensus process is created in proportion to the weight held by the account, so adding additional nodes to the model will not gain additional voting weight. In the DPoS-Quorum consensus, if a new consensus node wants to join the alliance chain, it must obtain the approval of the nodes in the existing alliance chain. Therefore, witch attacks are unlikely to succeed in either the PANDA consensus or the DPoS-Quorum consensus.

Distributed denial-of-service (DDoS) attack is a malicious attack that seeks to disrupt the normal traffic to the target server, service, or network by flooding the target or surrounding infrastructure with massive amounts of Internet traffic. The consensus proposed in this paper uses the verifiable random function (VRF) to calculate the legal consensus identity participating consensus secretly and locally. A node can only calculate its own identity secretly and locally. Such identify cannot be calculated in advance by other nodes, and other nodes can easily verify the legitimacy of the identity after the identity is broadcasted. The generation of consensus identity based on verifiable random function is non-interactive and posteriori, so it can prevent DDoS attacks. Since consensus identities cannot be acquired in advance, the malicious collusion between consensus identities is avoided.

3.4.3 Difference Between the Proposed Blockchain System and the Existing Blockchain System

Compared with the traditional Satoshi Nakamoto consensus algorithm, the PANDA algorithm is based on the DPoS consensus, which solves the problem of high energy consumption by selecting a legal identity to form a consensus committee. Compared with the traditional PBFT consensus algorithm, PANDA algorithm has a posteriori consensus identity, that is, randomly selected consensus committee members can prove their consensus identities without revealing their identities in advance. In addition, as the number of consensus nodes increases, there is no significant change in network bandwidth consumption. The latest rotation-based Algorand consensus algorithm lacks economic incentives, and has a large number of signature data, so it has strict requirements on network bandwidth. In contrast, the chain-based Ouroboros consensus algorithm is built in a highly synchronous network environment. Inspired by the blockchain Nano structure, public chain Alliance builds a Double-DAG structure. Compared with Nano, although the transaction processing speed and throughput are slightly lowered, the randomly selected consensus identity reduces the

risk of nodes being attacked by DDoS and the possibility of collusion between consensus nodes. In a highly synchronous network environment, consensus can be reached in a relatively short time.

4 Experiment and Simulation

In order to test the performance of the proposed algorithm, 30 virtual servers purchased from Aliyun, including 8 with 16 GB RAM CPU, were used in our experiment. The number of designed nodes in the public chain increased from 50 to 500, and the public chain based on PANDA consensus algorithm was developed in JAVA. A P2P network based on the Gossip protocol was deployed via IPFS. We stored all the experimental data for the transaction block in Oracle, the initial data in IPFS. The parameters of experiment are shown in Table 2.

4.1 Consensus Delay

The consensus delay in a blockchain system is the time it takes for a transaction to be created until it is initially accepted by the system. Using the public chain Alliance based on PANDA Consensus, if there is no bifurcate, the transaction can be approved by the system immediately. If there is a bifurcate, the consensus delay time mainly includes the consensus ID generation time and the consensus time. We designed Alliance-PBFT for consensus stage 1 and Alliance-PANDA for consensus stage 2. Figure 6 shows the consensus delay when only the consensus algorithm Alliance-PBFT is used. Light blue represents the time to generate consensus IDs, and dark blue represents the time to reach consensus. As the number of consensus nodes increases from 50 to 500, although the time to reach consensus is about 2 s, more time to generate consensus IDs, so the consensus delay time keeps rising.

For Alliance-PANDA, which has the same condition as Alliance-PBFT, the time to reach consensus is less than 2 s and the time to generate consensus IDs is basically unchanged. When the number of consensus node increased from 50 to 500, the proportion of shareholding was reduced from 200 to 20, and the consensus time is shown in Fig. 7. Some conclusions can be drawn by comparing Alliance-PBFT and Alliance-PANDA. First, before the number of consensus nodes exceeded 250, the consensus time in Alliance-PBFT was shorter than that in Alliance-PANDA, because the consensus messages

Table 2 Parameters used in simulation of public chain prototype system

Parameter	Definition	Value
f	safety parameter	10
Loyalt	The percentage of loyal users holding key licenses in the alliance chain	80%
Com-total	The size of steering committee in the public chain	200
Com-ExpCo	The number of expected consensus identities in steering committee in the public chain	200
ID-good	Threshold of honest identity	100
Max-vote	The maximum time of the voting period	30
XALT	Key license in alliance chain	12,000

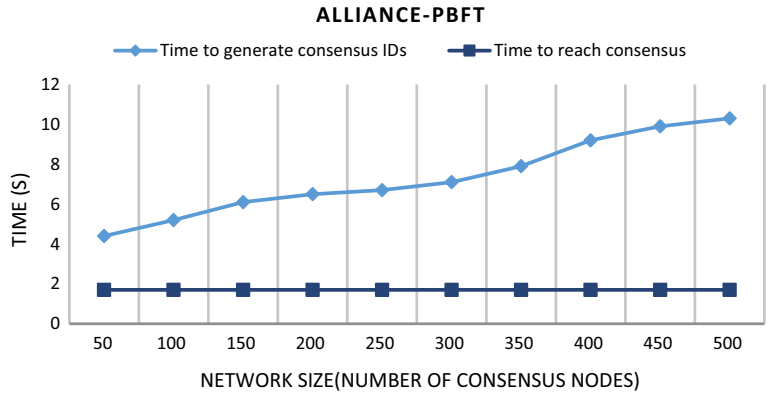

Fig. 6 Consensus delay when only the consensus algorithm Alliance-PBFT is used

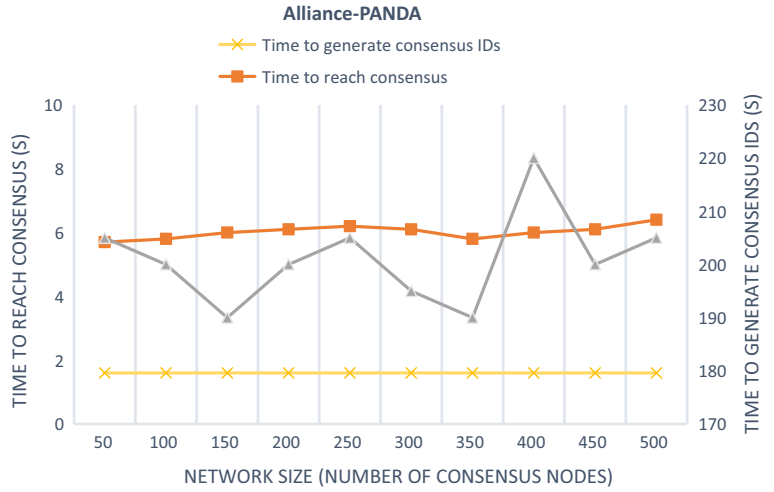

Fig. 7 Consensus delay when only the consensus algorithm Alliance-PANDA is used

in Alliance-PANDA were larger than those in Alliance-PBFT. Secondly, as the number of consensus nodes increased, it can be seen from the broken line in Fig. 7 that the number of identifies participating in consensus in the Alliance-PANDA algorithm varied around the expected value, while the number of consensus identities in the Alliance -PBFT algorithm continued to increase with the increase of nodes. As a result, the consensus time of Alliance-PANDA gradually became shorter than that of Alliance-PBFT, and the difference between the two modes became widened.

By comparing the Alliance algorithm (the Alliance-PBFT is adopted in the first stage, while the Alliance-PANDA algorithm is adopted in the second stage), Alliance-PBFT and Alliance-PANDA, we found that in the two stages, the time for nodes to participate in consensus almost did not change significantly with the increase in the number of nodes and tended to be stable. Compared with the traditional algorithm which shows significantly increased consensus time with the increase in number of nodes, the consensus time growth

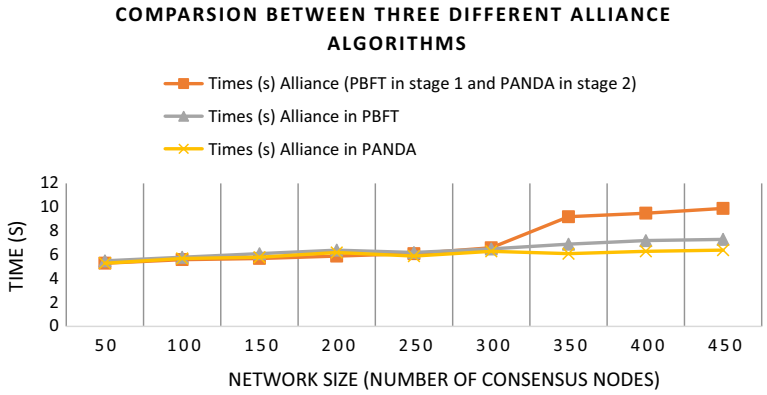

Fig. 8 Comparison of consensus delay when using PANDA algorithm, using only Alliance-PBFT and using only Alliance-PANDA

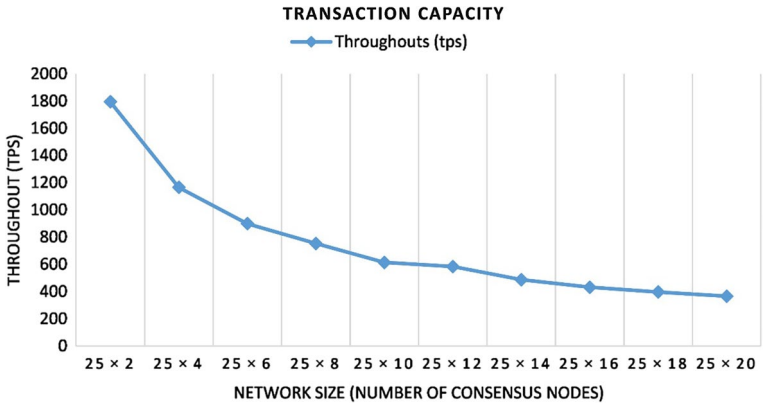

Fig. 9 Transaction throughput of the public chain Alliance

rate of Alliance algorithm was not so significant with the increase in number of nodes, so the proposed algorithm consumes shorter time and is more efficient, as shown in Fig. 8.

4.2 Transaction Capacity

In the transaction throughput experiment, we deployed a total of 500 nodes in the public chain, and the transaction block types include TBsend, TBreceive, and TBauth, whose transaction block size vary with the number of permissions. We collected the time required by 25,000 TBsend transactions. According to the throughput shown in Fig. 9, with the increase in the number of nodes, the throughput decreased continuously due to the limited hardware conditions. Although it cannot reach the theoretical value of 7000TPS, the throughput still reached 1200TPS when four Alliance nodes were deployed at the public chain (in fact, the cloud server is likely to deploy only one Alliance node at most), which is significantly larger than the transaction throughput (3TPS) in the Bitcoin network.

5 Discussion

5.1 Findings Related to Hybrid Chain Model

Balance among consensus efficiency, security and cost. In the hybrid chain structure, the consensus efficiency and transaction throughput are limited by the existing traditional blockchain structure. Therefore, this paper proposes a in current data management schemes, it is difficult for single chain structure to achieve an effective hybrid chain model combining PANDA (a consensus algorithm based on the public chain environment) and X-Alliance (a consensus algorithm based on the Alliance chain environment) to distributed store the encrypted sensitive data in the license chain. The attribute information of data is protected in the license chain, which not only reduces the cost of protection, but also periodically anchors the snapshot of the blocks in license chain onto the non-license chain, thus forming the chain-type trusted data protection mechanism. Finally, relevant experiments are designed to show that hybrid chain has the advantages of low consensus delay, high transaction throughput, high security and traceability. Moreover, in order to solve the conflict between throughput and fairness by similar algorithm [33] the whole network is divided into small regions, and each region is assigned a node according to its QoS. Subsequently, run deterministic Byzantine fault tolerance (BFT) consistency across all specified nodes. The designed hybrid chain model for trusted data in supply chain finance of engineering projects has a double-directed acyclic graph mechanism, which can process the transactions of each account in parallel, asynchronize from other unrelated accounts in the network, and theoretically improve the throughput of the model.

The engineering project data authentication model based on hybrid chain serves in the management of supply chain financial data of engineering project and helps to improve the phenomenon that financial institutions hesitate or refuse to lend loans. By encrypting and tracing the information chain of supply chain finance, small and medium-sized enterprises in the upstream and downstream of supply chain can conduct trade authenticity examination, risk assessment and credit transmission of core enterprises more efficiently, project participants can analyze and give early warning of capital flow, and timely analyze and calculate the authenticity of the transaction background, so as to provide a new method for normal operation of project funds under the novel coronavirus epidemic. Therefore, the proposed hybrid chain model is of great theoretical and practical significance.

5.2 Comparison with Other Scholars' Studies

The rapid development of supply chain finance, the combination of industry and finance, and the reduction of the overall operation cost of the supply chain have become the new ways for domestic enterprises and financial institutions to compete for innovation, providing a new way for precision marketing, intelligent decision-making and financial risk control. Li et al. [34] uses big data technology to analyze customers' browsing behaviors, habits and hobbies, so as to help enterprises understand customers' needs more clearly and provide customers with efficient and accurate services. With the help of "hologram", Yuan et al. [35] provides a new method to evaluate enterprise credit risk based on business behavior interaction. Although the emergence and application of emerging technologies such as the Internet of things and big data, supply chain finance can't be divorced from credit risk. In order to solve the regulation and actual implementation of a decentralized

system, Guo et al. [36] established "regulatory sandbox" and the development industry standards. The research of the three scholars analyzes the problem of enterprise trust risk from the aspects of understanding customer demand, business behavior, regulatory means, etc., but the causes of the risk are difficult to trace. Under the background of the increasing impact of the new crown epidemic on the global economy, we can't solve the problem of capital shortage and trust of core enterprises from the root. Compared with the above-mentioned scholars' research, this paper uses blockchain technology to put forward the method of credible data token, which makes the business behavior data of construction enterprises in the whole industrial chain ecology into "evaluable credit" and "negotiable assets". The token makes the potential investor base expand to a broader market, and then helps construction enterprises to be more effective, transparent and safer to carry out financial business.

5.3 Recommendations for Future Research

It is noted that a hybrid blockchain consistency algorithm proposed by [37] combines the advantages of PoS and PBFT algorithms to dynamically select consensus nodes in the form of verifiable password ordering. When 4 nodes are deployed in the experimental part, the throughput is lower than 1200TPS (the throughout of this algorithm), and the consensus delay time is about 3 s, which is longer than 2 s (consensus delay of this algorithm). Therefore, this algorithm has better performance than other similar algorithms.

Due to the limitation of time, there are still some deficiencies in this paper, and many studies have not been carried out in depth. However, these contents will also be the focus of future research work: (1) the algorithm can continue to improve, the efficiency of the algorithm can be enhanced; (2) the amount of sample data is increased, and the performance accuracy is further prompted. (3) This model is based on the application of supply chain finance scenario, and can further explore the application of other scenarios. The proposed hybrid chain model cannot support intelligent contracts at present, so it is not capable for more complex management of data assets. In addition, as for PANDA, the proposed consensus algorithm applicable to the public chain environment, if the consensus nodes fail to reach consensus in the first term, the identifies of members of the corresponding consensus committee will be exposed and vulnerable to attacks. Although the members of the consensus committee under attack will only affect the consensus of the corresponding bifurcate rather than affecting the consensus of other bifurcates, the prevention of attacks on the members of the consensus committee will remain the focus of the following work.

6 Conclusion

This work is carried out in the background of supply chain finance of engineering projects. Firstly, under the influence of the epidemic, the problems of SMEs' receivables increase, payment collection cycle is generally prolonged, financing is difficult and expensive, and the risk of default payment increases. In such circumstance, the industrial chain and supply chain exhibits "accumulation effect", capital chain of downstream departments suffers from a significant impact of risk, causing the higher percentage of daily volatility trading in small and medium-sized enterprises, rising risk of financial sector, inter-departmental transmission to other industries, resulting in significantly increased financial risks. This paper introduces the blockchain technology to ensure the authenticity and reliability of the

original data and to transform the data assets lacking market liquidity into the pass-through that can be freely traded in the financial market. On this basis, it can reduce the reliance of core enterprises on credit support, reduce verification cost and overcome information asymmetry in supply chain transactions, so that more enterprises can participate in the design of supply chain financial products.

To solve the problem of data security, a consensus algorithm PANDA based on public chain environment is proposed. Compared with the alliance chain and the private chain, the public chain shows higher decentralization degree, higher trust degree and higher security degree, and the cost of breaking the system is enormous. Therefore, the consensus algorithm PANDA based on the public chain environment has higher data security. Aiming at the problem of long consensus delay and low cost in blockchain system, a consensus algorithm X-Alliance is proposed. Alliance chain has more reliable nodes and controllable network environment, so it has extremely fast transaction speed, better privacy protection and lower transaction cost.

Acknowledgements The research was supported by the Guangdong University Students' Scientific and Technological Innovation Foundation (No. pdjh2021b0406), Humanities and Social Sciences Project of Ministry of Education (No. 20YJCZH097), Guangdong Planning Office of Philosophy and Social Sciences (No. 2020GZGJ185). The authors would like to acknowledge the valuable suggestions of the editors and the anonymous reviewers.

References

1. Association. C.C.I. (2020). Investigation Report on How Covid-19 Impacted the Chinese Construction Enterprise. Available online: http://news.hexun.com/. Accessed on 05 March 2020.
2. Wu, C. F. M. C. (2020). Credit guarantee mechanism with information asymmetry: a single sourcing model. *International Journal of Production Research, 58*(16), 4877–4893. https://doi.org/10.1080/00207543.2020.1727039.
3. Fu, Y. G., & Zhu, J. M. (2019). Big production enterprise supply chain endogenous risk management based on blockchain. *IEEE access, 7*, 15310–15319. https://doi.org/10.1109/ACCESS.2019.2895327.
4. Schmidt, W. (2015). Supply chain disruptions and the role of information asymmetry. *Decision Sciences, 46*(2), 465–475. https://doi.org/10.1111/deci.12133.
5. Saberi, S., Kouhizadeh, M., Sarkis, J., & Shen, L. G. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research, 57*(7), 2117–2135. https://doi.org/10.1080/00207543.2018.1533261.
6. Azzi, R., Chamoun, R. K., & Sokhn, M. (2019). The power of a blockchain-based supply chain. *Computers & Industrial Engineering, 135*, 582–592. https://doi.org/10.1016/j.cie.2019.06.042.
7. Han, K. M., Park, S. W., & Lee, S. (2020). Anti-fraud in international supply chain finance: Focusing on moneual case. *Journal of Korea Trade, 24*(1), 59–81. https://doi.org/10.35611/jkt.2020.24.1.59.
8. Tung, J. K., & Nambudiri, V. E. (2018). Beyond Bitcoin: Potential applications of blockchain technology in dermatology. *The British Journal of Dermatology, 179*(4), 1013–1014. https://doi.org/10.1111/bjd.16922.
9. Hughes, A., Park, A., Kietzmann, J., & Archer-Brown, C. (2019). Beyond Bitcoin: What blockchain and distributed ledger technologies mean for firms. *Business Horizons, 62*(3), 273–281. https://doi.org/10.1016/j.bushor.2019.01.002.
10. Drljevic, N., Aranda, D. A., & Stantchev, V. (2020). Perspectives on risks and standards that affect the requirements engineering of blockchain technology. *Computer Standards & Interfaces, 69*, 103409. https://doi.org/10.1016/j.csi.2019.103409.
11. Yang, F., Zhou, W., Wu, Q. Q., Long, R., Xiong, N. N., & Zhou, M. Q. (2019). Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism. *IEEE Access, 7*, 118541–118555. https://doi.org/10.1109/ACCESS.2019.2935149.
12. Mohsin, A. H., Zaidan, A. A., Zaidan, B. B., Albahri, O. S., Albahri, A. S., Alsalem, M. A., & Mohammed, K. I. (2019). Blockchain authentication of network applications: Taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions. *Computer Standards and Interfaces, 64*, 41–60. https://doi.org/10.1016/j.csi.2018.12.002.

13. Nawari, O. N., & Ravindran, S. (2019). Blockchain and the built environment: Potentials and limitations. *Journal of Building Engineering, 25*, 100832. https://doi.org/10.1016/j.jobe.2019.100832.
14. Bamakan, S. M. H., Amirhossein, M., & Alireza, B. B. (2020). A survey of blockchain consensus algorithms performance evaluation criteria. *Expert Systems with Applications, 154*, 113385. https://doi.org/10.1016/j.eswa.2020.113385.
15. Cardoso, R. C., & Bordini, R. H. (2017). A multi-agent extension of a hierarchical task network planning formalism. *Advances in Distributed Computing and Artificial Intelligence Journal, 6*(2), 5–17. https://doi.org/10.14201/ADCAIJ201762517.
16. Benisi, N. Z., Aminian, M., & Javadi, B. (2020). Blockchain-based decentralized storage networks: A survey. *Journal of Network and Computer Applications, 162*, 102656. https://doi.org/10.1016/j.jnca.2020.102656.
17. Bhattacharya, R., White, M., & Beloff, N. (2017). A blockchain based peer-to-peer framework for exchanging leftover foreign currency. *IEEE*. https://doi.org/10.1109/SAI.2017.8252284.
18. Cao, B., Li, Y. X., Zhang, L., Zhang, L., Mumtaz, S., Zhou, Z. Y., & Peng, M. G. (2019). When internet of things meets blockchain: Challenges in distributed consensus. *IEEE Network, 33*(6), 133–139. https://doi.org/10.1109/MNET.2019.1900002.
19. Gao, Y. F., Kawai, S., & Nobuhara, H. (2019). Scalable blockchain protocol based on proof of stake and sharding. *Journal of Advanced Computational Intelligence and Intelligent Informatics, 23*(5), 856–863. https://doi.org/10.20965/jaciii.2019.p0856.
20. Xu, G. X., Liu, Y., & Khan, P. W. (2020). Improvement of the DPoS consensus mechanism in blockchain based on vague sets. *IEEE Transactions on Industrial Informatics, 16*(6), 4252–4259. https://doi.org/10.1109/TII.2019.2955719.
21. Xu, L. D., & Viriyasitavat, W. (2019). Application of blockchain in collaborative internet-of-things services. *IEEE Transactions on Computational Social Systems, 6*(6), 1295–1305. https://doi.org/10.1109/TCSS.2019.2913165.
22. Sungbin, L., & Kim, K. H. (2020). Design of enhanced PoS mechanism for scalability without centralized process. *The Journal of Korean Institute of Next Generation Computing, 16*(1), 75–85.
23. Mazières, D. (2015). The Stellar Consensus Protocol: A Federated Model for Internet-Level Consensus. https://www.stellar.org/papers/stellar-consensus-protocol.
24. Sylim, P., Liu, F., Marcelo, A., & Fontelo, P. (2018). Blockchain technology for detecting falsified and substandard drugs in distribution: Pharmaceutical supply chain intervention. *Jmir Research Protocols, 7*(9), e10163. https://doi.org/10.2196/10163.
25. Bolt, W. (2017). Bitcoin and cryptocurrency technologies: A comprehensive introduction. *Journal of Economic Literature., 55*(2), 647–649. https://doi.org/10.1257/jel.55.2.644.
26. Mohsin, A. H., Zaidan, A. A., Zaidan, B. B., Albahri, O. S., Albahri, A. S., Alsalem, M. A., & Mohammed, K. I. (2019). Based blockchain-PSO-AES techniques in finger vein biometrics: A novel verification secure framework for patient authentication. *Computer Standards & Interfaces, 66*, 103343. https://doi.org/10.1016/j.csi.2019.04.002.
27. Ouaguid, A., Abghour, N., & Ouzzif, M. (2018). A novel security framework for managing Android permissions using blockchain technology. *International Journal of Cloud Applications and computing, 8*(1), 55–79. https://doi.org/10.4018/IJCAC.2018010103.
28. Kaushik, S., & Gandhi, C. (2019). Ensure hierarchal identity based data security in cloud environment. *International Journal of Cloud Applications and computing, 9*(4), 21–36. https://doi.org/10.4018/IJCAC.2019100102.
29. Sumathi, M., & Sangeetha, S. (2020). Blockchain based sensitive attribute storage and access monitoring in banking system. *International Journal of Cloud Applications and computing, 10*(2), 77–92. https://doi.org/10.4018/IJCAC.2020040105.
30. Esposito, C., Ficco, M., & Gupta, B. B. (2021). Blockchain-based authentication and authorization for smart city applications. *Information Processing and Management, 58*(2), 10. https://doi.org/10.1016/J.IPM.2020.102468.
31. Li, D. M., Deng, L. B., Gupta, B. B., Wang, H. X., & Choi, C. (2019). A novel CNN based security guaranteed image watermarking generation scenario for smart city applications. *Information Sciences, 479*, 432–447. https://doi.org/10.1016/j.ins.2018.02.060.
32. Nedjah, N., Wyant, R. S., Mourelle, L. M., & Gupta, B. B. (2019). Efficient fingerprint matching on smart cards for high security and privacy in smart systems. *Information Sciences, 479*, 622–639. https://doi.org/10.1016/j.ins.2017.12.038.
33. Yu, B., Liu, J., Nepal, S., Yu, J. S., & Rimba, P. (2019). Proof-of-QoS: QoS based blockchain consensus protocol. *Computers & Security, 87*, 101580. https://doi.org/10.1016/j.cose.2019.101580.

34. Li, L., Chi, T., Hao, T. T., & Yu, T. (2018). Customer demand analysis of the electronic commerce supply chain using Big Data. *Annals of Operations Research, 268*(1–2), 113–128. https://doi.org/10.1007/s10479-016-2342-x.
35. Yuan, G. X. Z., & Wang, H. Q. (2019). The general dynamic risk assessment for the enterprise, by the hologram approach in financial technology. *International Journal of Financial Engineering, 6*(1), 1950001. https://doi.org/10.1142/S2424786319500014.
36. Guo, Y., & Liang, C. (2016). Blockchain application and outlook in the banking industry. *Financial Innovation (Heidelberg), 2*(1), 1–12. https://doi.org/10.1186/s40854-016-0034-9.
37. Wu, Y. Q., Song, P. X., & Wang, F. X. (2020). Hybrid consensus algorithm optimization: A mathematical method based on POS and PBFT and its application in blockchain. *Mathematical Problems in Engineering, 11*, 1–13. https://doi.org/10.1155/2020/7270624.

Jingkuang Liu received the B.S. degree from Yichun College, Jiangxi, China, in 2006, the M.S. degree from Guangzhou University, Guangzhou, China, in 2010, and Ph.D. degree from South China University of Technology, Guangzhou, China, in 2013. He is currently Associate Professor of Guangzhou University, Guangzhou, China. His research interests include Automation in Construction, Blockchain technology application, Construction Management and Economics.

Lemei Yan was born in Henan, China, in 1995. She is a post-graduate student and pursuing for master degree. Her research interests include Automation in Construction, Blockchain technology application, Construction Management and Economics.

Dong Wang received the B.S. degree from Hainan University, Haikou, China, in 2006, the M.S. degree from Guangdong University of Technology, Guangzhou, China, in 2008, and Ph.D. degree from Jinan University, Guangzhou, China, in 2013. He is currently a Lecturer of Guangzhou University, Guangzhou, China. His research interests are Business Intelligence, Data Mining, Information Systems and Behavior Economics.