EasyChair Preprint

№ 1393

Byzantine fault-tolerant coalition chain consensus algorithm for protection of electricity information

Zhaohui Zhang, Jinggang Yang, Jun Jia, Chengbo Hu, Ziquan Liu, Yang Xu and Fengbo Tao

August 12, 2019

Byzantine fault-tolerant coalition chain consensus algorithm for protection of electricity information

Zhaohui Zhang, Jinggang Yang, Jun Jia, Chengbo Hu, Ziquan Liu, Yang Xu, Fengbo Tao
State Grid Jiangsu Electric Power Co., Ltd. Electric Power Research Institute
Electric Power Research Institute
Nanjing, China
e-mail: 363680788@qq.com

***Abstract*—Based on the credit model's Byzantine fault-tolerant coalition chain consensus algorithm and neural network construction node credit model, this paper improves the practical Byzantine fault-tolerant algorithm based on the credit model and proposes a Byzantine fault-tolerant consensus based on credit model algorithm.**

Keywords-power information protection; alliance chain; consensus algorithm; Byzantine fault tolerance

I. INTRODUCTION

Smart grids improve the efficiency, reliability, and economy of the grid in an automated manner to optimize grid management and operations. With the mature application of intelligent measurement technology, more accurate, convenient, budget power meter reading, and real-time monitoring meter reading greatly improve the efficiency of power meter reading. It enables the power companies to adjust the power supply more scientifically and quickly to optimizes the balance between supply and demand between power supply and power consumption. It also effectively avoids redundant power generation while meeting the basic power consumption of power users. However, too frequent uploading of power data will cause serious personal privacy leaks to users. The data uploaded by the smart meter can be used by the unscrupulous person, which may cause the leakage and tampering of users' electricity information, personal sensitive information and the trade secret information, resulting in the loss of the users or the power companies, thus posing a threat to the users and power companies.

With the development of communication technology, the close integration of communication technology and smart grid makes two-way communication based on grid possible. The smart meter, which plays an important role between the users and grids, becomes a direct terminal for two-way communication and providing an interactive experience for the users. The smart meter collects the power consumption information of smart device. When the power consumption changes, the power consumption, time, and other information will be uploaded to the power companies in real time, then the power companies will distribute and predict the power consumption. Smart meter relies on intelligent measurement technology.

The three types of main privacy data in the smart meter environment include identity information of a smart meter for uniquely identifying a home or a user; user consumption information for real-time uploading to a power company, that is, smart meter real-time power data; and the total power consumption information of the users that need to be uploaded in a certain period, that is, the total power consumption data of the smart meter. If the unlawful person obtains the unique identifier of the smart meter and the power consumption data of users uploaded by smart meter in real time, they can attack the users. Research on the use of electricity information protection for user in smart grids is still in its infancy.

As an emerging technology, blockchain is a decentralized distributed ledger technology realized by deep integration of distributed technologies, consensus algorithms, cryptography, peer-to-peer networks, etc., it provides a credible channel for information and value transfer in a de-trusted environment [1]. The federated blockchain is referred to as the coalition chain, it is targeted to specific groups. Only authorized nodes can join a specific blockchain network. Nodes in the coalition chain need to be authenticated and registered in advance. The consensus process usually does not involve encryption. The member nodes have common goals, but they do not fully trust each other in maintaining transaction data. Compared with the public blockchains, the coalition chain nodes usually have good connections, high verification and confirmation speed, faster time to release, and lower system maintenance costs. Combined with the latest technological developments in blockchains, the coalition chain can realize the internal member to be responsible for the maintenance of the book, and the registration mechanism can limit the behavior of the participating nodes, flexible authority processing, and to some extent, construct a decentralized and distributed system, and get rid of the single system. It gets rid of the security risks caused by a single point of failure brought by a single central organization. And it also solves the problem of trust. It can be applied to current financial, supply chain, public welfare and other application scenarios. It has very important practical significance especially in the privacy protection of smart grids. As a key technology in the coalition chain, the consensus algorithm directly affects the transaction processing capability, scalability and security of the coalition chain. This paper proposes a credit model-based

Byzantine fault-tolerant coalition chain consensus algorithm for power information protection [2]. The algorithm builds a node credit model based on BP (back propagation) neural network. Based on the credit model, it improves the PBFT (Practical Byzantine Fault Tolerance). A credit-based Byzantine Fault Tolerance (CBFT) algorithm for power information protection is proposed.

II. COALITION CHAIN CONSENSUS ALGORITHM

The consensus problem has always been an important research topic in the distributed field. According to the different ways of selecting the block accounting node, the consensus algorithm can be roughly divided into the following four categories [3]: Including proof-like consensus algorithms such as Proof of Work (PoW) and Proof of Stake (PoS) [4]. Broadcast electoral consensus algorithms such as Raft algorithm. Rotating consensus algorithms such as PBFT. Hybrid consensus algorithms Such as PoS + BFT. PoW and other algorithms have problems such as severe waste of energy consumption, low throughput, and prolonged transaction time. As a classic implementation of Byzantine fault-tolerant algorithm, PBFT algorithm is of great significance to the coalition chain. It is the core support of the coalition chain consensus algorithm. Many coalition chain consensus algorithms are inspired by it and improved for specific scenarios.

Miguel Castro and Barbara Liskov proposed the PBFT algorithm in 1999, which can provide 1/3 fault tolerance under the premise of ensuring activity and security, and reduce the complexity of BFT algorithm from exponential to polynomial, this makes BFT algorithm feasible in practical system applications. Then on the basis of this classic PBFT algorithm, the researchers have done a lot of improvement work. It mainly includes Quorum-based algorithms with Query/Update and Hybrid/Quorum as the typical, Speculation-based algorithms with Zyzzava as the typical and client-based algorithms with OBFT (Obfuscated BFT) as the typical. The above algorithms are designed to simplify the PBFT algorithm for different scenarios without errors. Therefore, when encountering Byzantine errors, the performance of such algorithms generally declines to varying degrees, and it is even difficult to ensure the activity of the system [5].

In addition, the PBFT algorithm is based on the principle of State Machine Replication and consists mainly of a coherence protocol, a view switching protocol, and a checkpoint protocol. Under normal circumstances, the system runs under the consistency protocol and checkpoint protocol. When the master node fails, the view switch protocol will be started to ensure that the system executes the client request in an orderly manner [6]. This is a scenario for a typical distributed database. The request is input to the system at a very high frequency, and the system may perform thousands of consensus processes in 1 second. Once a timeout occurs, the slave nodes in the system consider the master node to be a Byzantine node, so in this scenario, the Commit phase is required to improve consensus efficiency. But in an coalition chain chain system, it is usually a few minutes or even longer to agree on a block. If there is a problem with the block, it directly agrees that the default block with a block is empty, instead of rolling back, so the Commit phase is not needed [7]. In addition, in the PBFT algorithm, the replacement of the master node is generated in turn, which is risky. If several consecutive replica nodes elected as the master node are Byzantine, the availability of the system is greatly reduced.

III. TECHNICAL SOLUTIONS

A. Building a Blockchain Node Credit Model Based on BP Neural Network

When the election mode of the primary node is changed, the PBFT algorithm adopts the method of selecting the primary node in turn. In this way, the malicious primary node is elected to cause the view to be replaced, resulting in greatly reduced system performance. Therefore, this paper proposes a credit-based master node election, based on BP neural network to construct a blockchain node credit model, select the highest credit node to be elected as the master node, thus reducing the probability of the Byzantine node as the main node, making the view replacement times greatly Reduced, system performance is improved. BP neural network is a kind of multi-layer neural network based on error back propagation algorithm. It can flexibly model the sample data and reveal the implicit nonlinear relationship. It is suitable for constructing node credit evaluation model. The credit model evaluation system adopted in this paper designs 8 evaluation indicators according to the integrity level and performance of the nodes in the consensus process, which is used as the input of BP neural network, as shown in Table I.

TABLE I. NODE EVALUATION INDEX

Number	index	Indicator interpretation
1	Network delay time	Node network delay time
2	The number of nodes offline	Number of offline nodes of the blockchain system
3	Node offline time	Record the time when the node is offline
4	Not participating in the number of times	The number of online slave nodes that failed to participate in the new block uplink update because of the Byzantine node
5	New block winding time	The average of each round of new block verification and execution to the winding time
6	Node join network time	The time the node participates in the system
7	Whether to provide invalid blocks	The master node is a Byzantine node that may provide invalid blocks
8	Node credit	The credit value of the node in the previous round

In the node credit evaluation element, it includes network delay time, node offline time, number of times of non-participation, number of offline nodes, time of uplink of new block, time of node joining network, availability of invalid block, node credit value, etc. data. The data used in this algorithm are all non-negative, but because the dimension of each evaluation index is large, the sample data needs to be normalized to map to the [0,1] interval and then used as the input of the BP neural network model. The input layer of the credit model designed by this algorithm includes 8 neurons. The input represents the network delay time, the number of offline nodes, the offline time of the node, the number of times the uplink is not involved, the time of the new block, the time of joining the network, the invalid block, and the node credit; the output layer contains 1 neuron. ; The hidden layer is designed as one layer, and the number of hidden layer neurons is generally determined by empirical method or trial and error method.

B. CBFT algorithm flow

Transaction request sending phase: Transaction initiator C broadcasts the transaction to the whole network, and attaches the sender's signature. All the consensus nodes independently listen to the transaction data of the whole network, verify the legality of the transaction, and cache it if it is legal; the primary node collects enough transaction requests or, after a certain time interval, packages the requests into blocks.

Proposal stage: The primary node generates a proposal message and signs the newly generated block. The message format is: $\langle \text{PROPOSE}, \nu, \text{n,p, p,D(block)} \rangle \sigma p$, ν is the view number, n is the number of the block request, p is the main node serial number, and the block hash that needs consensus is described as a summary: D(block). After the slave node receives the new block proposal, it needs to verify the legality of the proposal. When an illegal transaction or invalid block is found, the "dishonest behavior" is recorded to the node status record table, the consensus is abandoned, and a view replacement protocol is initiated; when the slave node is verified and confirms that the proposal information sent by the master node is correct, it enters the confirmation phase.

Confirmation phase: After the node enters the confirmation phase, it broadcasts an $\langle \text{CONFIRM}, \nu, \text{n,p,D(block),i} \rangle \sigma i$ message to other slave nodes. i is the node's own serial number, and receives confirmation messages from other nodes. Check the message signature, summary, view number is correct, etc. If it passes, it will be cached. When the slave node receives more than the consistent information from 2*f*+1 different nodes, the node enters the confirmation phase, executes the block transaction, and replies to the $\langle \text{REPLY}, \nu, \text{t,n,c,i,r} \rangle \sigma i$ message to the client. Where *t* is the timestamp, *n* is the block number, *c* is the client, *i* is the number of node *i*, *r* is the reply of node *i*, and σi is the signature of node *i* on the message.

When the client receives a reply message of more than *f*+1 nodes, and their reply has the same timestamp *t* and reply *r*, the consensus is reached, and each node performs the block winding.

C. Improved view replacement protocol

When the slave node detects that a timeout is detected or the master node has an error, a view change message is broadcast to all nodes in the blockchain system network, and the view replacement message format is $\langle \text{VIEW-CHANGE}, \nu+1, \text{L,Q,i} \rangle \sigma i$. *L* is the sequence number of the node with the highest credit value selected according to the node credit ranking table, and *Q* stores the request set information of all completed PROPOSEs of the node *i* in the previous view. After receiving the VIEW-CHANGE message, the node verifies that the signature of the message, the view, the new primary node sequence number *L*, and the *Q* set information are legal. If they are legal, they send $\langle \text{VIEW-CHANGE-ACK}, \nu+1, \text{i,j,d} \rangle \sigma i$ to the new master node. If the new master node receives 2*f*+1 VIEW-CHANGE messages, it will select the nearest checkpoint, calculate the sequence number corresponding to the block request according to the Q set, and finally encapsulate it into the $\langle \text{VIEW-CHANGE}, \nu+1, \text{V,X} \rangle \sigma p$ message and broadcast it. V contains the VIEW-CHANGE message sent by other slave nodes and the corresponding VIEW-CHANGE-ACK message set. *X* identifies the selected checkpoint and request value.

After receiving the new-view message sent by the new *v*+1 node, the slave verifies the message signature and whether the message is repeatedly processed, and re-assigns the block summary for each sequence n according to the *V* set and the *X* set. At the same time, it is verified whether the result of the assignment is consistent with the allocation result in the NEWVIEW message sent by the master node (verification message digest). When it is consistent, the data state of the current node is synchronized to the checkpoint time point position, and then the *X* set is traversed to generate message information.

The follow-up consensus is the consensus processing flow of the classic PBFT algorithm.

IV. SIMULATION VERIFICATION

A. Throughput test

This consensus algorithm is mainly for the coalition chain. Therefore, the Hyperledger Fabric is used as the blockchain framework, and the CBFT algorithm is used as the consensus algorithm. The system is compared with the Hyperledger Fabric v0.6 open source framework using the PBFT consensus algorithm. Transaction throughput is the rate at which a blockchain network submits valid transactions within a defined time. It is expressed in transaction per second (TPS) and can be expressed as:

$$\mathrm{TPS} = \frac{T_{\Delta t}}{\Delta t} \tag{1}$$

where $T_{\Delta t}$ represents the total amount of transactions in the block time and Δt represents the block time. For the simulation analysis of the model, we consider the measurement data at a single point. The size of the block will affect the throughput. The larger the block, the larger the network bandwidth and the corresponding delay will increase. Therefore, in order to control the variables for comparison, we set the MaxMessages item in one block to 20. Three sets of controlled experiments of CBFT consensus algorithm and PBFT consensus algorithm were tested under 4, 5 and 6 consensus nodes. Multiple tests were averaged to obtain statistical results, as shown in Figure1.

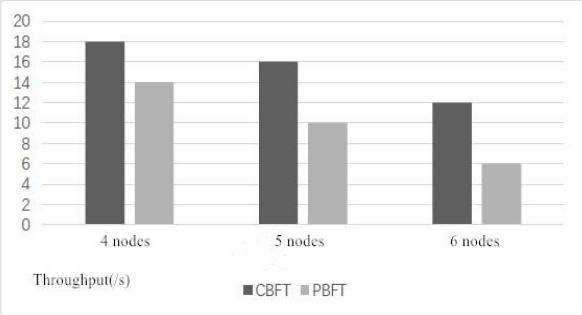

Figure 1. Comparison of throughput between CBFT and PBFT

It can be seen from Figure 1 that as the number of nodes increases, the throughput of both CBFT and PBFT algorithms decreases, but the throughput of CBFT is higher, and the throughput reduction rate is smaller than that of PBFT with the number of nodes. This is because the adoption of the credit model reduces the number of view replacements, so communication consumption and delay caused by operation rollback and the like are reduced, and the throughput of the blockchain system is increased.

B. Delay test

The delay test in a blockchain system usually refers to the time interval from the submission of a transaction to the confirmation of a submission. In the performance test of this paper, in order to compare with the performance of PBFT, it is simplified to the consensus delay test, that is, the time when the block proposal is broadcast to the completion of the block consensus. Consensus delay is an important indicator to measure the speed of the consensus algorithm. The smaller the delay, the faster the transaction is confirmed.

$$T_{\text{delay}} = T_{\text{conform}} - T_{\text{propose}} \tag{2}$$

where T_{conform} is the block consensus completion time, and T_{propose} is the main node to start broadcasting the proposal time. The average value of multiple tests is obtained, and the consensus time difference between the CBFT consensus algorithm and the PBFT consensus algorithm is obtained, as shown in Figure 2:

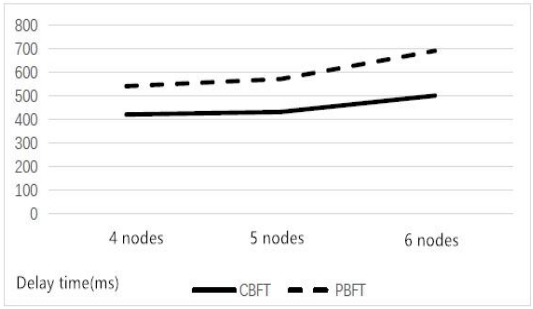

Figure 2. Comparison of consensus delay between CBFT algorithm and PBFT algorithm

It can be concluded from the above figure that the number of view replacements is reduced because of the adoption of the credit model, so that the communication consumption and delay caused by the operation rollback and the like are reduced, and the delay of the blockchain system is reduced.

C. Security analysis

Experiments show that the CBFT consensus algorithm reduces communication overhead, increases throughput, and reduces the consensus delay of the block based on the classical PBFT algorithm, ensuring the consistency and security of the distributed system of blockchain. And, like PBFT algorithm provides fault tolerance $f = \frac{n-1}{3}$.

In the CBFT algorithm consensus process, if the number of Byzantine nodes in the system is less than 1/3, when the master node propagates a malicious request or the master node is down, the system changes the view and reselects the next node with the largest credit value. Consensus under the premise of ensuring system security and activity. When more than 1/3 of the cases exceed the maximum number of Byzantine nodes that the system can withstand, the consensus cannot be completed.

V. CONCLUSION

Based on the consistency protocol and view replacement protocol of PBFT algorithm, this paper proposes a model-based Byzantine fault-tolerant CBFT consensus algorithm. Due to the node credit model, the number of view changes is greatly reduced. Therefore, the coherence protocol omits the COMMIT phase of PBFT, which greatly reduces the node traffic, reduces the block confirmation time, and speeds up the transaction confirmation.

VI. ACKNOWLEDGEMENT

This work is supported by Project Supported by Science and Technology Foundation of SGCC (Grant No.: 5210EF18000W), and State grid Jiangsu electric power co. LTD. science and technology project funding (Grant No.: 5210EF18001C).

REFERENCES

[1] Yong Yuan, Feiyue Wang. Development Status and Prospect of Block Chain Technology [J]. Journal of Software, 2016, 42(4):481-494.

[2] Androulaki E, Barger A, Bortnikov V, et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains[J], 2018.

[3] Lamport L. The Part-Time Parliament[J]. ACM Transactions on Computer Systems 19Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains98, 16(144-169).

[4] Sunny K, Scott N. Ppcoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake[J]. self-published paper, 2012, 19.

[5] Juels A, Burton S. Kaliski J. Pors: Proofs of Retrievability for Large Files[C]. Proceedings of the 14th ACM conference on Computer and communications security, Alexandria, Virginia, USA, 2007:584-597.

[6] Shao Qifeng, Jin Chengqing, Zhang Zhao, et al. Block Chain Technology: Architecture and Progress [J]. Journal of Computer Science, 2018, 40(425):3-22.

[7] Yuan Yong, Ni Xiaochun, Zeng Shuai, et al. Development status and Prospect of block chain consensus algorithm [J].Journal of Automation, 2018, 44(11):2011-2022.

AUTHORS' BACKGROUND

Your Name	Title*	Research Field	Personal website
Zhaohui Zhang	Engineer	Power transmission and transformation project commissioning and power system overvoltage analysis and detection work	
Jinggang Yang	Senior Engineer	Research on testing and testing technology of electrical equipment	
Jun Jia	Engineer	Power artificial intelligence technology and overvoltage analysis	
Chengbo Hu	Senior Engineer	Electric power Internet of things technology, equipment state intelligent diagnosis technology work	
Ziquan Liu	Engineer	Development of key technologies for intelligent operation and inspection of electric power	
Yang Xu	Senior Engineer	Power equipment fault diagnosis and dc transmission	
Fengbo Tao	Senior Engineer	Overvoltage and transformer technology related work	