A New Consensus in Bank Liquidation System

Jiang-lei GUI, Xiao ZHANG, Fa-guo WU and Wang YAO* 
School of Mathematics and Systems Science, Beihang University, Key Laboratory of Mathematics, Informatics and Behavioral Semantics, Ministry of Education, Beijing, 100191, China

*Corresponding author

Keywords: Consensus, Blockchain, Liquidation system.

Abstract. Blockchain serving as an unalterable ledger, has received widespread attentions recently, which allows carrying out transactions with a decentralized matter. Applications with blockchain technology are springing up. However, financial applications especially in bank liquidation system are still facing big challenges. This paper first presents a consensus combined delegated-proof-of-stake protocol and BFT algorithm together. At the same time, using parallel idea and redesigned blockchain structure make the system more efficiency.

Introduction

With the development of banking, the ability to liquidate and pay is the key to test the bank's normal operation. Based on the actual needs of bank, bank’s understanding of liquidation and payment ability has become the key to guarantee the development of banks. However, from the current operation of the bank's modern settlement and payment system, the system itself still exists some problems. Traditionally, in the bank liquidation process, the transaction and settlement of funds are separated and each bank keeps accounting separately. With the transaction completed, both banks have to spend a large quantity of manpower and resources to reconcile them, because the data is recorded by the opponent and both parties can’t confirm the authenticity of this data fluently. What’s more, with the case that both banks don’t have mutual accounts, an authoritative third party is needed to help complete the liquidation process, which absolutely yield additional costs. And this phenomenon still exists extensively in the real world [1][2].

Recently, cryptocurrency has received significant attentions in both academia and industry. First of all, Bitcoin, has shown a different way to architect value exchange on the Internet [3][4][5]. With being the most successful cryptocurrency, one bitcoin is approximately equivalent to 8300 dollars in November 2017 and has enjoyed a huge success [6]. The core technologies of Bitcoin are blockchain and the Nakamoto consensus. Blockchain seems like a public ledger and all valid transactions are committed and stored in chain block, which become longer and longer as new blocks are created and appended to the chain continuously. With the proof-of-work mechanism, the Nakamoto consensus works by selecting one processor every 10 minutes which solved a puzzle problem and issues a proposal that all the other members adopts. At the same time, Asymmetric cryptography has been implemented in the blockchain for user security. The main purpose of creating Bitcoin is to remove third parties and reduce transaction costs, because Trading has come to rely seriously on financial institutions regarded as trusted third parties with electronic payments, which increases transaction costs and is non-reversible. Therefore, using the blockchain technology in bank liquidation system has become a very natural idea. After using blockchain technology, the transaction information of both banks is recorded on the blockchain network which can’t be tampered with and real-time liquidation can be completed. This eliminates the cumbersome data exchange and liquidation work and funds utilization efficiency can be greatly improved.

Unfortunately, the throughput of the Bitcoin network is not scaling well, which consumes plenty of computation power. And compared to 2000 transactions per second in centralized payment system, the Bitcoin network which is restricted to a rate of 7 transactions per second is incapable of dealing with high frequency trading [7]. Actually, for this problem, some scholars have proposed new
consensus mechanisms like proof-of-stake and Delegated-proof-of-stake\textsuperscript{[8]}\textsuperscript{[9]}. However these new consensus are still facing some serious problem. For instance, the proof-of-stake mechanism makes the rich one get richer while the security of Delegated-proof-of-stake mechanism seriously dependents on the delegate.

The key idea of this paper is to combine the Delegated-proof-of-stake mechanism and a Byzantine consensus algorithm together. On the one hand, it can solve the security of delegate in the Delegated-proof-of-stake system. On the other hand, using parallel idea makes the Byzantine consensus more efficient. Eventually, this paper puts forward a new consensus protocol for better use in bank liquidation system with blockchain technology.

**Consensus design**

In this section, we present a new consensus protocol. Firstly, we define the components of the new protocol. Secondly, we highlight the threat model and security assumptions. Finally, we show an overview of the protocol and describe each step of the protocol in detail.

**Protocol Components**

Server: A server represents a bank or client. The clients only send and receive funds, which can’t participate in the consensus process. On the contrary, the banks must participate in the consensus process.

Normal group: A member in the normal group just takes part in the consensus within the group, which has no right to append the transaction to the blockchain.

Final group: A member in the final group is responsible for the final consensus and adds a valid transactions to the blockchain.

Block: The block is regarded as a ledger, which is a record of the Clients’ valid transactions and is repeatedly updated with transactions that successfully pass through the consensus process.

**Threat Model and Security Assumptions**

 Mostly, a bad bank server is regarded as a threat model, which is a byzantine node with arbitrarily malicious behavior. Security assumptions and more details can refer to\textsuperscript{[10]}.

**The New Consensus Protocol**

The protocol proceeds in epochs. In each epoch, bank server executes the following steps:

Step 1. All the bank servers which want to participate in the system must solve a puzzled problem with local computation.

Step 2. Yield m (a prescribed constant) bank servers to make up the final group by anonymous election from the banks which solved the puzzled problem. The others are randomly assigned to the normal group also with m members.

Step 3. Each member in the same group communicates to discover identities of others in their group.

Step 4. Bank servers in one normal group run an authenticated Byzantine agreement protocol within their group to agree on a single value\textsuperscript{[11]}\textsuperscript{[12]}. Each group sends the selected value (signed) to the final group.

Step 5. Bank servers in the final group compute a final value with all the values received from normal group, and broadcast the final result.

In Step1, each server generates an identity of the form (IP, PK). In order to participate in the consensus process, each bank has to solve a proof-of-work. That is to say they must find a valid nonce satisfying the inequality:

\[
O = H(R \| PK \| IP \| nonce) < D. \tag{1}
\]

In (1), PK is a public key and IP and PK are selected by each bank server, which will be disclosed to the network. H is a hash function and randomness R is produced by final group in a specific time. D
is a parameter to control the difficulty of solving the problem. For instance, D can be a bunch of binary numbers with 40 leading zeros. The reason why we set a proof-of-work to participate in the consensus process is that can resist Sybil attack \cite{13}. Therefore, the difficulty of our problem doesn’t need to reach the same level of Bitcoin in order to avoid bringing too much resource consumption.

In Step 2, after solving the puzzled problem, there is a passed server list. The bank servers will make an anonymous vote on the list and the top c is regarded as the member of final group. As we all know, the selected banks must be powerful and responsible with high probability, which is beneficial to the entire system. However, the list of final group is not immutable, because the anonymous vote will be conducted periodically. The remaining part of the list are assigned by final group to a random normal group with a group identity, even for the adversary, which shouldn’t have capability to bias normal group assignment with non-ignorable probability.

In Step 3, once normal groups are established, group members must to create point-to-point connections mutually. Instead of communicate with the entire server, normal members can contact with the final group to announce their group identity. Then the final group member will give a member list of the same normal group. In this way, normal group members can contact with each other within the group easily.

In Step 4, each normal group executes an internal group consensus protocol to reach a consistent value. The value is signed by the group members with at least c/2 + 1 signatures. Then the group sends the signed value to the final group members. When the signatures can’t reach c/2 + 1, the selected value is invalid, then the internal group consensus is repeated.

In Step 5, each final member validates the values which are sent by each normal group member and takes an ordered set union to create a cryptographic digest. Then, the final group run the same consensus algorithm to ensure the result is indeed correct. When getting at least c/2 + 1 signatures from the final group members, the entire network can verify it.

**Structure Design**

In this section, we first review the structure of the Bitcoin blockchain. Then combined with the above consensus mechanism, we present our own block structure.

In Bitcoin blockchain, each data block generally contains two parts: block header and block body. The block header encapsulates the current version number and contains the address of the previous block, the current target bits, the nonce, Merkle root and Timestamp \cite{14}. The block body consists of all the transactions in a period. These transactions generate a unique Merkle root by the hash function and the Merkle root is recorded on the block head as we said above. And the structure of Bitcoin blockchain shown in Figure 1.

![Figure 1. The structure of Bitcoin blockchain.](image)
A Merkle tree is a binary hash tree, which leaf node stores hash of transaction and internal node is a hash value of children nodes. There, all the transactions will be stored in a hash value by Merkle root and from Merkle root we can prove the existence of all the transactions.

So with solving the consensus algorithm and learning the essential blockchain structure well, we can design our blockchain with new consensus mechanism in bank liquidation process. As we shown in Figure 2 and Figure 3, we devise two blockchains design which include final blockchain and normal blockchain [15]. The structure of normal blockchain is mostly like the Bitcoin’s, which contains last block address, final block address, timestamp, Merkle root of all the transactions, the normal group id and signatures. A transaction here means that bank a paid a sum of money to bank B like a fee paid from Bob’s ICBC credit card to the BOC account of business. However, the normal block isn’t broadcast to the entire network immediately. On the contrary, the final block will be broadcast immediately when a valid final block is created, which includes the last block address, timestamp, final group signatures and normal block address without transactions. As we all know, a server can check the validity from the final group signatures and if someone care about the data of the transactions, he can get the normal block address from the final block.

![Figure 2. The structure of final block.](image1)

![Figure 3. The structure of normal block.](image2)

**Potential Advantages and Future Work**

When considering DPoS consensus mechanism as the protocol in bank liquidation system, the security always relies on the delegate’s loyalty. Thus, our protocol combined DPoS and BFT algorithm together solve the problem of delegate loyalty. At the same time, with using parallel idea, the whole consensus process is shortened. While traditional BFT algorithm have to reach consensus with plenty of nodes, normal group reach consensus at the same time then the final consensus is achieved with c members. What’s more, the entire system will be optimized with two blockchains.
With one blockchain, more useless information could participate in the whole process, which could influence the efficiency of the whole system. However, in fact only the most recent blocks keep data useful for the trading and the information of the final block is enough for final consensus.

With these advances, here we still have numerous studies to do. When adopting a new protocol and structure in bank liquidation system, the transaction rate is still facing with some challenges. Thus, we have to make further optimizations for the system. And when it comes to bank transaction, users’ privacy is regarded as a serious problem. The transaction should only be used by those who need it and the idea of homomorphic encryption should be adopted to protect users’ privacy better[16][17]. What’s more, two blockchains must cause more resource consumption although in this way the efficiency of the system will be improved. So the balance among them is also worth further thought.

Conclusion

After learning the main consensus algorithm in blockchain technology, we found that existing consensus mechanism and bank liquidation system can’t be matched well. Therefore, we present a new protocol that combines delegated proof-of-stake and BFT together to solve the problem of delegates’ loyalty. And this paper use parallel idea and new structure of blockchain to improve the consensus efficiency. At the same time, we adopt a weakened proof-of-work method to protect the system from Sybil attack.

Reference

[1] Cooper R., Kempf H. Deposit insurance and bank liquidation without commitment: Can we sleep well? [J]. Economic Theory, 2016, 61(2): 365-392.
[2] Mason J.R., Anari A., Kolari J.W. The speed of bank liquidation and the propagation of the U.S. Great Depression [J]. Proceedings, 2000, 61(2): 523-524.
[3] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system [J]. Consulted, 2008.
[4] Information on https://en.wikipedia.org/wiki/Ripple_%28payment_protocol%29.
[5] Information on https://en.wikipedia.org/wiki/Litecoin.
[6] Information on https://cn.investing.com/currencies/btc-usd-converter/.
[7] Eyal I., Gencer A.E., Sirer E.G., et al. Bitcoin-NG: A Scalable Blockchain Protocol [J]. 2015: 45-59.
[8] King S., Nadal S. PP_coin: Peer-to-Peer Crypto-Currency with Proof-of-Stake [J]. 2012.
[9] Information on https://bitshares.org/technology/delegated-proof-of-stake-consensus/.
[10] Luu L., Narayanan V., Baweja K., Zheng C., Gilbert S., Saxena P., SCP: a computationally-scalable Byzantine consensus protocol for blockchains. Cryptology ePrint Archive, Report 2015/1168.
[11] Dolev D, Strong H R. Authenticated Algorithms for Byzantine Agreement [J]. Siam Journal on Computing, 1983, 12(4): 656-666.
[12] Attiya C., Dolev D., Gill J., Asynchronous Byzantine Agreement. Proc. 3rd. Annual ACM Symposium on Principles of Distributed Computing. 1984.
[13] Douceur J.R. The Sybil Attack [C]/International Workshop on Peer-to-Peer Systems. Springer, Berlin, Heidelberg, 2002: 251-260.
[14] Information on https://en.wikipedia.org/wiki/Merkle_tree.
[15] Tsai W.T., Blower R., Zhu Y., et al. A System View of Financial Blockchains [C]// Service-Oriented System Engineering. IEEE, 2016: 450-457.

[16] Herrera-Joancomartí J., Pérez-Solà C. Privacy in Bitcoin Transactions: New Challenges from Blockchain Scalability Solutions [M]// Modeling Decisions for Artificial Intelligence. Springer International Publishing, 2016.

[17] Information on https://en.wikipedia.org/wiki/Homomorphic_encryption.