A Permissioned Blockchain Framework for Supporting Instant Transaction and Dynamic Block Size

Xinping Min[1,3], Qingzhong Li[1,2(✉)], Lei Liu[1], Lizhen Cui[1,3]
[1] School of Computer Science and Technology, Shandong University, Jinan, China
[2] Dareway Software Co.,Ltd, Jinan, China
[3] Electronic Commerce Research Center of Shandong University, Jinan, China
lqz@sdu.edu.cn

***Abstract*—The lack of credibility of transactions has become major issue restricting the rapid development and popularization of E-commerce. Existing solutions adopt blockchain protocols to improve the credibility of transactions. Most of them still have significant scalability barrier, such as instant transaction and throughput. By analyzing how fundamental and circumstantial bottlenecks in Bitcoin-derived blockchain limit the ability of its current peer-to-peer overlay network, this paper presents Permissioned Blockchain Framework (PBF). PBF aims at achieving trusted trading and supporting instant transaction in E-commerce. To guarantee a higher credibility of transactions, this paper presents a global consensus algorithm - Permissioned Trusted Trading Network Consensus Algorithm. In order to fulfill the demand of instant transactions without sacrificing credibility, this paper presents a Peer Inner Blockchain Protocol. The comparison between PBF and Bitcoin-derived blockchain in E-commerce, suggests better performance on throughput, latency, capacity.**

Keywords—Blockchain; consensus algorithm; trusted transaction

I. INTRODUCTION

E-commerce becomes more and more popular in our life, although there are many major issues to be addressed, such as the lack of credibility of transaction. Due to all related information are kept on trading platform, and provided services are massively centralized, resulting in both strict control by the central bodies or vulnerability used by criminals. As a result of this, only trading center, such as Tmall, has permission to provide related information or credibility. If a trading center suffers from network attacks, it's easy for a trading center to be tampered transactions. Due to privacy information on current E-commerce platform, the government is inconvenient to attain statistics information. If it adopts one blockchain protocol to improve the credibility of transaction, it will cause privacy disclosure of transactions and a lower throughput. So, to demonstrate better performance on E-commerce, improving the blockchain becomes a major issue to be addressed.

A blockchain [1] is a transaction database shared by all nodes participating in a network based on a consensus protocol. With this mechanism, each node can find out how many transactions belonged to each node at any point in history. One of this technical features [2] is that it enables reliable transactions without a centralized management mechanism even if there are unreliable participants or adversary in the network, and this feature is obtained by the invention of blockchain protocol. Due to adopting a gossip p2p architecture, another great technical feature of blockchain is that each peer stores a complete public ledger. The information of transaction can be accessed by every peer. By using this mechanism, blockchain can decentralize the credibility. Moreover, every block contains a hash of the previous block and a hash of current block, which has an influence on creating a chain of blocks from the previous block to the current block. These properties make the double-spending difficult, and public data to every participant.

The Bitcoin-derived blockchain holds great promises for distributed ledgers, but this blockchain protocol cannot have better performance on E-commerce. Bitcoin-derived blockchain can solve the lack of credibility of transactions, but doesn't demonstrate better performance on throughput, capacity and latency. The Bitcoin-derived blockchain is a gossip protocol so that all state modifications to the ledger must be broadcast to all participant node. If the amount of transactions grows rapidly, meaning that bandwidth increases as a square of the number of nodes in terms of bandwidth overload. Due to Bitcoin-derived blockchain adopting full replication mechanism, each node must store a copy of all blocks. As the amount of blocks grows, only those with the resources to hold all the blocks will be able to participate. Moreover, each block takes 10 minutes to process, as a result, Bitcoin-derived blockchain cannot support instant transactions. However, afore mentioned properties have no efficient impact on E-commerce.

In E-commerce, each transaction must be immediately processed, and massive transactions occur simultaneously. In Bitcoin-derived blockchain, the block size is currently 1MB, and subject to only 1 to 3.5 transactions per second [3]. If E-commerce adopts Bitcoin-derived blockchain protocol to solve problems, it cannot deal with massive transactions, and will increase the cost of network communication. So, this paper presents a Permissioned Blockchain Framework (PBF) to guarantee a higher credibility of transactions. Without sacrificing higher credibility, PBF can keep unlimited data and

2324-9013/16 $31.00 © 2016 IEEE
DOI 10.1109/TrustCom.2016.49

support instant transactions. The goal of PBF is to construct a higher credibility, public, autonomous E-commerce ecosystem.

The key idea in PBF is to partition the network into sub-committees, where the membership of each committee is linear in the total computation power of the network. Each sub-committee runs a peer inner consensus protocol to process a separate set of transactions and blocks. To do that partition, PBF leverages a random partition algorithm, which can limit dishonest peer and securely split peers in the network into subcommittees. Special committee agrees on peer's blocks, consisting of a set of valid transactions. Another Special committee is designated to write peer's blocks into a global block, so that each peer can find out how many transactions or blocks belonged to each peer at any point in history. In this mechanism, PBF can guarantee a higher credibility.

Our goal is to ensure that the framework offers the same level of security as Nakamoto consensus, but with a higher throughput and a lower latency. PBF includes three parts: Permissioned Trusted Trading Network Consensus Algorithm (PTTNCA), a Peer Inner Blockchain Protocol (PIBP), and an E-commerce blockchain architecture. E-commerce Blockchain Architecture is a three-layer blockchain, and can keep unlimited transactions without sacrificing higher credibility. PIBP is a collaborative protocol to improve the throughput and support instant transactions, without wasting too much computation resources. PTTNCA leverages proof-of-work mechanism to generate global blocks in every epoch. PTTNCA can guarantee that any micro block of peers can be find in other peers. Some blockchain protocols use a set of validation peer to validate the legality of transactions, but all of those blockchains consider the validation peer always valid. PTTNCA includes a validation peer selection algorithm, which can dynamic change membership of validation set in each epoch.

Unlike Bitcoin, [4] is an anonymous payment system that can provide excellent blockchain privacy and higher throughout. However, the parties entrusted to anonymize transactions in [5] can still violate users' anonymity, even if they are honest-but-curious. PBF can protect users' anonymity without sacrificing higher credibility. Ittay Eyal [6] presents Bitcoin-NG, a new Bitcoin-derived blockchain protocol designed to scale. Bitcoin-NG achieves that Byzantine fault tolerant, robust to extreme churn, and sharing the same trust model obviating qualitative changes to the ecosystem. But Bitcoin-NG still have limitation on throughput and latency. PBF supports instant transactions with a lower latency and a higher throughput.

The contributions of our research are two-fold:

- A Permissioned Blockchain Framework in E-commerce. This paper represents a Permissioned Blockchain Framework, which has better performance on E-commerce. PBF can guarantee a higher credibility of transaction, support instant transaction, and keep unlimited data.
- Higher throughput and lower latency: Permissioned Blockchain Framework can significantly achieve a higher throughput and lower latency than Bitcoin-derived blockchain while maintaining the same trust assumptions.

The remainder of the paper is organized as follow: Section II introduces the related work about blockchain scalability. In Section III, this paper provides the overview of Permissioned Blockchain Framework. Section IV describe the Permissioned Blockchain Framework in detail. Section V introduces the experiment about Permissioned Blockchain Framework. The conclusion of PBF in Section VI

II. Related Work

Bitcoin-derived blockchain is a distributed, distributed ledgers, which implicitly defined and implemented the Nakamoto consensus. Despite its potential, Bitcoin-derived blockchain protocols face a significant scalability barrier. For example, the maximum rate at which these systems can process transactions is capped by the choice of two parameters: block size and block interval. Increasing block size can improve throughput, but the causing bigger blocks that take longer time to propagate in the network. Reducing the block interval can reduce latency, but leads to instability that the chain is forked into branches. To improve efficiency, one has to trade off throughput for latency. So, blockchain protocol has scalability issues in terms of throughput, latency, capacity, and communication cost [7].

There is a lot of work that to improve throughput, reduce latency and communication cost. For example, Andrew Miller [8] introduces AddressProbe, a technique that discovers peer-to-peer links in Bitcoin. By analyzing the measured Bitcoin network topology, AddressProbe presents both high degree nodes and a well-connected giant component to improve throughput. Christian Decker [9] presents off-blockchain transactions. It is possible to create long-lived channels over which an arbitrary number of transfers can be processed locally between two nodes, without any burden to the Bitcoin network. Ittay Eyal presents Bitcoin-NG, a new Bitcoin-derived blockchain protocol designed to scale. Bitcoin-NG achieves that Byzantine fault tolerant, robust to extreme churn, and sharing the same trust model obviating qualitative changes to the ecosystem. Andrew Miller [10] presents a formal model of synchronous processes without distinct identifiers that communicate using one-way public broadcasts. Adam Back [11] proposes a new technology, pegged sidechains, which enables Bitcoins and other ledger assets to be transferred between multiple blockchains. By reusing Bitcoin's currency, these systems that based on Bitcoin, can more easily interoperate with each other and with Bitcoin, avoiding the liquidity shortages and market fluctuations associated with new currencies. Juan Garay [12] proposes and analyzes applications that can be built "on top" of the backbone protocol, specifically focusing on Byzantine agreement and on the notion of a public transaction ledger. Hong-Jie He [13] proposes a blockchain based fragile watermarking scheme to solve the issue of security and accuracy of tamper localization. In the proposed scheme, all blocks randomly form a linear chain based on the secret key in such a manner that the watermark of a block is hidden in the next block in the block-chain.

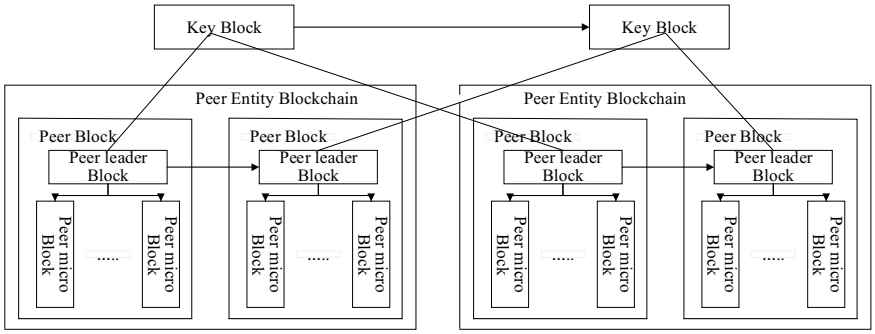

Figure 1: Permissioned Trusted Blockchain Architecture

Yoad Lewenberg [13] proposes an alternative structure to blockchain that allows for transactions at much higher rates. This structure consists of a directed acyclic graph of blocks. The proposed model allows blocks to reference multiple nodes, and allows for more "forgiving" transaction acceptance rules that incorporate transactions even from seemingly conflicting blocks. Evan Duffield [15] develops a new privacy centric cryptographic currency based on Satoshi Nakamoto's Bitcoin, Darkcoin can send anonymous blocks transactions directly into the node using extensions to the core protocol and use an improved proof-of-work mechanism, which using a chain of hashing algorithms replaces the SHA256 algorithm and result in a slower encroachment of more advanced mining technologies.

There is a lot of work to improve the blockchain, most of those cannot improve the throughput, latency and credibility of transactions at the same time. And most of those sacrifice the privacy of transactions and throughput. This paper presents a Permissioned Blockchain Framework to have significant impact on E-commerce, with a higher credibility, higher throughput and lower latency.

III. Permissioned Trusted Blockchain Protocol Overview

Definition 1: Peer. Each peer represents a third-party trading platform, such as Tmall. A peer contains a cluster of computation node. Computation nodes have permission to generate blocks and transactions. Each peer must have a unique identification, such as a public key and a private key. Each peer has itself blockchain to keep itself transactions. Each peer also keeps other peer's block header into itself blockchain. Each block of peer must have other peer's signature, so that the transactions in block can become legal.

Definition 2: Entity. An entity represents a buyer or seller in E-commerce. Each entity can commit a transaction across any peer. Each entity must have a unique identification in the whole network, such as a public key and a private key. All entities' identification must be kept on in each peer.

Definition 3: Permissioned Trusted Trading network (PTTN). Multiple peers compose PTTN based on Permissioned Blockchain Framework. PTTN introduces three types of peer: construction peer (CP), validation peer (VP), regular peer (RP). Each kinds of peer has permission to generate itself blocks and transactions. Only a CP can have permission to generate global block in PTTN, which contains all hash of peer's block in an epoch. Only a VP can decide a block whether is valid or invalid. PBF don't allow any peer to have construction and validation permission simultaneously.

Definition 4: Permissioned Trusted Blockchain Architecture (PTBA). As shown as in Figure 1, PTBA introduces four types of blocks: peer block, key block, peer leader block, micro block. Each block or transaction goes from undecided to decided valid or decided invalid. Each block has a header that contains the unique reference of its predecessor, namely a cryptographic hash of the predecessor header. A key block contains multiple peer blocks. A peer block contains a peer leader block and multiple micro blocks. A peer leader block contains multiple micro block's hash value. A micro block contains specific transactions that occurred in one peer.

Permissioned Blockchain Framework (PBF) contains three parts: peer inner blockchain protocol (PIBP), permissioned trusted trading network consensus algorithm (PTTBCA) and permissioned trusted blockchain architecture.

PBF can serialize transactions, support instant transactions and support dynamic block size, without sacrificing the higher credibility. In each epoch, firstly, each peer writes transactions into their micro blocks. Meanwhile, according to peer's honesty that indicates the probability of tampering transaction, available mining power that indicates peer's computation power, PBF randomly generates construction and validation peer set. Each peer sends their micro blocks to validation peer set, and validation peers validate the legality of micro blocks. Second, each peer generates peer block, and sends their peer blocks to validation and construction peer set. A construction peer set competitively generates key block, and sends key block to validation peer set. Third, validation peer set decides this key block whether is valid. If this key block is valid, validation peer set sends this block to the remained peers. Once there is majority of negative (invalid) votes for a key block, each validation peer deletes this key block, reduces that peer's honesty which generated the latest key block, and wait for next key block. At last, validation peer set generates a new construction and validation peer set for next epoch.

IV. Permissioned Trusted Blockchain Protocol

A. Peer Inner Blockchain Protocol

In this section, we will describe the peer inner blockchain protocol. To improve the throughput of transactions and the

latency, this paper presents a Peer Inner Blockchain Protocol (PIBP).

In PIBP, when a peer generates a micro block, this peer sends this micro block to the validation peer set. When a micro block comes in, it gets validated by validation peers. If any validation peer agrees on this micro block, this peer writes the vote into this block and sends this micro block to the next validation peer. If there is majority of positive (valid) vote for a peer micro block, all validation peer write this block into peer's blockchain. This paper proposes that a recipient of the signature micro block generates a new block referring to the received micro block, which represents intention of consenting to it. Once there is majority of positive (valid) votes for a peer micro block, the peer micro block goes from undecided to decided valid, respectively, and the process of voting on the block stops. Only the valid peer micro block can be wrote into peer leader block. Only a micro block can be retrieved in any peer leader blocks, the micro block can be considered legal.

The hash function of micro block or peer leader block replaces timestamp with random number. Each block must be signed a signature by constructor. The size of micro block isn't bounded by a predefined maximum. If a micro block comes from the future, this micro block is considered invalid.

Suppose this situation, a dishonesty peer tampers the previous transactions and replaces the hash value of all related blocks in itself blockchain. The tampered transaction has no signature with validation peers, and other peers cannot find the hash value of tampered blocks in any key block. So those transactions wrote in tampered block are not valid or legal.

To improve the latency, all peers only send the blocks header, and all validation peers adopt vote mechanism to validate the legality of blocks. To improve the throughput, multiple computation nodes collaboratively generate one peer block. In PIBP, each peer block is divided into multiple micro blocks and one peer leader block. PIBP divides computation node into multiple groups, each group collaboratively generates a micro block, a final group collaboratively generates a peer blocks. In each group, each computation node has a Transaction Database (TD) and a Peer Block Database (PD). TD takes in and assigns incoming transactions, and PD holds ordered transactions that are 'etched into stone'. Every computation node in one group shares the same data in TD and PD.

Now, according to the distribution of computation node's mining power, PIBP divides all computation node into multiple groups. We can write threshold of sum of mining power in one group as:

$$P_{mean} = \sigma^2 \bullet (P_{max} + P_{min}) \tag{1}$$

P_{mean} represents threshold of sum of mining power in one groups, P_{max} represents the maximum mining power of all computation node, P_{min} represents the minimal mining power of all computation node, σ^2 represents the variance of computation node mining power's normal distribution.

PIBP uses greedy algorithm [16, 17] to calculate the number of group K. The number of computation nodes in each group should be almost equal. We define optimization goal as follows:

$$\begin{cases} P_{mean} - \beta \le R\_group_j \le P_{mean} + \beta, 1 \le i, j \le K \\ |num\_group_i - num\_grorup_j| \le \eta, 1 \le i, j \le K \\ \max(\sum_{j=1}^{K} R\_group_j) \end{cases} \tag{2}$$

CN_i represents i-th computation node in a peer. R_CN_i represents i-th computation node's available mining power, a limited amount of computing power. P_{mean} represents the sum mining power of one group. N_p represents the number of computation node of a peer. R_group_j represents the sum of all computation nodes mining power in j-th group, $1 \le i, j \le K$. num_grorup_j represents the number of computation node in j-th group, $1 \le i, j \le K$.

As shown in Algorithm 1, computation node grouping algorithm can be divided into two steps: firstly, the algorithm roughly divides all computation nodes into multiple groups, and assigns computation node into each group. Secondly, according to optimization goal, this algorithm changes the number of group, and refines the membership of each group.

B. Permissioned Trusted Trading Network Consensus

This section introduces the global consensus algorithm that can prevent dishonest peer and guarantee a higher credibility of transactions.

In PTTN, CP not only has permission to generate key block, but also has permission to generate itself blocks and transactions. In other words, it's a greater possibility that CP can tamper transactions. By constructing validation and construction peer set, this paper presents a permissioned trusted network consensus algorithm to improve the higher credibility of transactions.

In PTTNCA, when a peer generates a peer leader block, the peer sends peer leader block header to VP and CP set. When a CP generates a key block, this CP sends the key block to all validation peers. VP set validates the hash value of each peer block in key block whether is tampered. As soon as there is majority of positive votes for a key block, or a majority of negative votes, the key block goes from undecided to decided valid or decided invalid, respectively. And the process of generating key block stops.

At the end of each epoch, current VP set generates next CP and VP set, and sends this information to the remained peers. But if one peer doesn't receives the information of next CP and VP set, this peer still sends itself blocks to the previous CP or VP set. Because each VP or CP just works in an epoch, previous CP or VP cannot deal with those blocks. The solution as follows: when a peer receives a key block, checks the key block whether contains hash of blocks belonged to itself. If all key block in an epoch don't contains some blocks, or the waiting time beyond the threshold, the peer sends those blocks again in next epoch.

At the end of each epoch, VP or CP still has some blocks to be processed. In this situation, all VPs and CPs stop right now,

and drop all blocks that have not to be processed or are processing. Those peers will send the blocks in next epoch. The latency of this mechanism have negligible implication on performance — it adds several milliseconds.

Algorithm 1 Peer Entity Grouping Algorithm

Input: Distribution of computation node's mining power
Output: group_i : Each group

1: Install the number of group K=$\left\lfloor (\sum_{i=1}^{N_p} R\_CN_i) / P_{mean} \right\rfloor$
2: CN_list represents Descending sorted result by mining power.
3: For i=1:length(CN_list)
4: index = $i\%K$
5: If $\text{R}\_group_{index} < P_{mean} + \beta$
6: Add $CN\_list(i)$ into $\text{group}_{(i\%K)}$
7: Remove $CN\_list(i)$ from CN_list
8: End If
9: End For
10: Deal with group which $\text{R}\_group_{index} < P_{mean} - \beta$
11: For i=1:K
12: If $\text{R}\_group_i < P_{mean} - \beta$
13: Select minimal item Item_j from CN_list
14: Add Item_j into group_i
15: End if
16: End For
17: If $(\sum_{i=1}^{N}\sum_{j=1}^{N}|\text{num\_group}_i - \text{num\_grorup}_j|) / 2\eta \geq N$
18: K=K+1
19: Remove the minimal item from CN_list
20: Go to step 3
21: Else if $(\sum_{i=1}^{N}\sum_{j=1}^{N}|\text{num\_group}_i - \text{num\_grorup}_j|) / \eta > N$
22: and $(\sum_{i=1}^{N}\sum_{j=1}^{N}|\text{num\_group}_i - \text{num\_grorup}_j|) / 2\eta \leq N$
23: K=K - 1
24: Remove the middle item from CN_list
25: Go to Step 3
26: Else
27: Compare R_group_i with each other.
28: If $\text{R}\_group_i - \text{R}\_group_j > \text{P}_{max} - P_{min}$
29: Refine the membership of $group_i$ and $group_j$
30: End If
31: Output group_i
32: End if

When one CP generates key block in the first time, this CP sends this key block to all validation peers. Each VP receives this key block, and validates whether all hash value of key block as same as received. If majority of validation peers agree this key block is valid, validation peers send this key block to remained peers. Other peers receive and keep this key block. If majority of validation peers agree this key block is invalid, it indicates the CP tampers some information, and this CP is dishonest. We must reduce the honesty value of that CP, and all validation peers remove this key block and wait for another key block.

Algorithm 2 CP and VP set generating algorithm

Input: Each Peer's information
Output: ConstructionList : CP set
ValidationList : VP set
1: some VPs using rank function get the rank result STN_P
3: Send STN_P to other validation peers
4: All validation peer check STN_P
5: If majority of peer agree STN_P
6: Send STN_P to the remained peer
7: Else
8: Select another VP to recalculate STN_P
10: Go to step 1
11: End If
12: For i=1:length(STN_P)
13: If $\sum_{i=1}^{num} Rank\_P_i < sum(R\_P) / 5$
14: Add R_P_i into ConstructionList
15; End if
16: End for
17: Divided remained peer into different $Pgroup$
18: For i=1:length($Pgroup$)
19: Select one membership in $Pgroup_i$
20: Add this peer into ValidationList
21: End for
21: Send ValidationList to current and next construction peers
22: All construction peer check ValidationList
23: If majority of peer agree ValidationList
24: Send ValidationList to the remained peers
25: Output ConstructionList and ValidationList
26: Else
27 Select another validation peer to recalculate ValidationList
28: Go to step 18
29: End If

Now, the punishment function for dishonest peer as follows:

$$H\_P_i = H\_P_i^{-NumTamperInfo} \quad (3)$$

H_P_i represents the i-th peer sorted by peer's honesty value. $NumTamperInfo$ represents the number of information that i-th peer tampered.

Then, the peer rank function as follows:

$$Rank\_P_i = \alpha \bullet R\_P_i + \lambda \bullet \text{H}\_P_i \quad (4)$$

$Rank\_P_i$ represents i-th peer rank. R_P_i represents i-th peer's available mining power. α represents the weight of R_P_i, λ represents the weight of H_P_i.

According to available mining power and honesty value of each peer, PTTNCA generates CP and VP set. As shown in algorithm 2, CP and VP set generating algorithm can be divided into two steps: firstly, we construct construction peer set by rank function. Secondly, we construct validation peer set by selecting form different group.

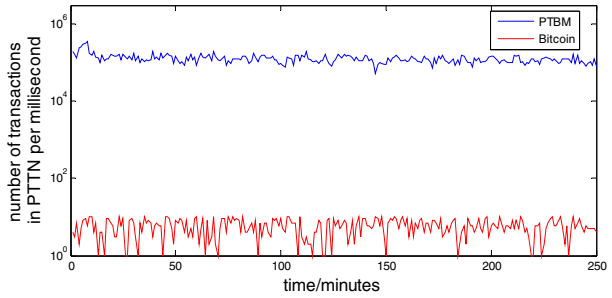

Figure 2: the number of transactions per millisecond

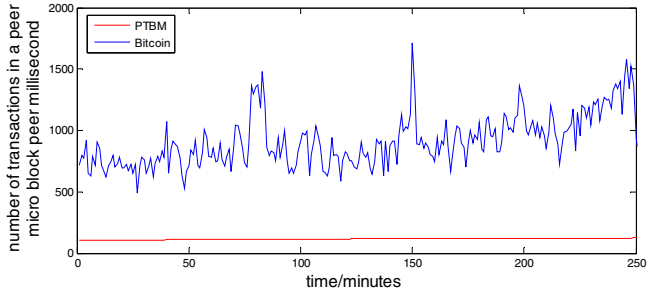

Figure 3: the number of transactions in each peer micro block per millisecond

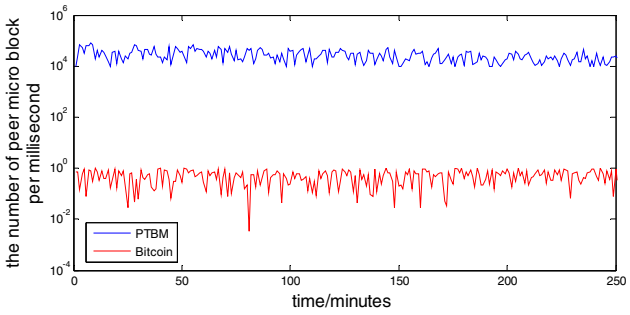

Figure 4: the number of peer micro block in Trusted Trading network

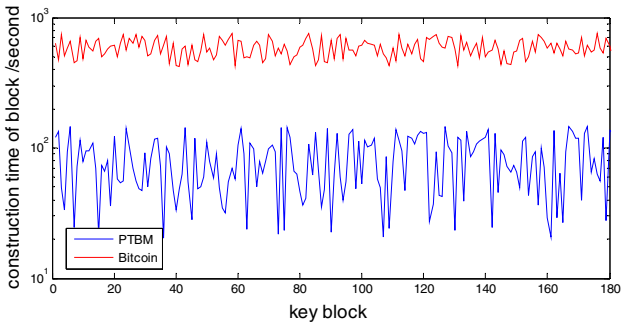

Figure 5: the key block constructed time.

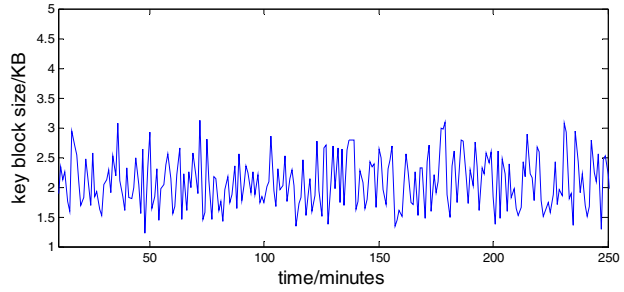

Figure 6: key block size

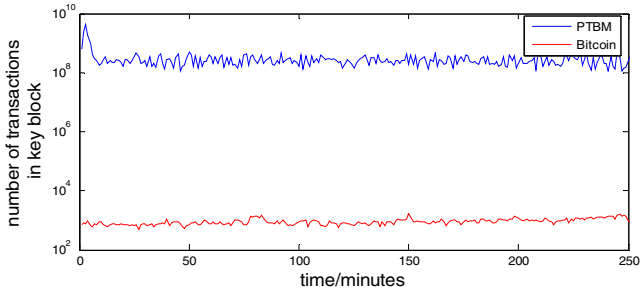

Figure 7: number of transactions key block contains

In the beginning, there is no CP and VP set in PTTN. It's a crucial problem how to initial the construction and validation peer set. Because VP set can generate the CP set. So, this paper presents an initial VP set algorithm. Initial validation peer set algorithm can be divided into two steps: firstly, each peer generates validation peer set by combining rank function with a random number, writes it into a block. Secondly, all peers validate the received block until majority of peers agree one block is valid.

V. Experimental Evalutions

In this section, we evaluate Permissioned Blockchain Framework (PBF) with 1000-node experiments on an emulated network. This paper did not implement the micro block's signature check. This elements have negligible implication on performance — signature checking adds several milliseconds. All the experiments are implemented on ten Intel Core i5 CPU 3.20 GHz machine with 8G of memory running Windows 10.

When generating blocks at high frequencies, the overhead of filling in the blocks by generating and propagating transactions becomes a dominant factor with Bitcoin's current implementation. This is an inherent property of Bitcoin-derived protocol, or of a blockchain protocol in general. But, in PBF, it's better to propagate the header of blocks, so there is no transactions propagation. PBF writes some external information in the header of blocks, so that other peers can validate the legality of blocks.

We evaluate PBF and compare it with Bitcoin in three sets of experiments, throughput of transaction, block frequency and block size. On same assumptions, PBF qualitatively outperforms Bitcoin, as it suffers no such deterioration, while enjoying superior performance in almost all metrics across the entire measured range.

A. Throughput of Transactions

First, we run experiments targeted at improving the throughput of transactions. Bitcoin adopts the proof-of-work consensus mechanism, the throughput of transactions is lower than 10 per second with consuming too much computation power. In PBF, figure 3 shows that up to million transactions per millisecond in Trusted Trading network, rather than a few transactions in Bitcoin network. As we can see from Figure 2, up to 10000 micro blocks per second in PBF, rather than one block about ten minutes in Bitcoin network. As we can see

from Figure 3, the number of transactions in each micro block up to 10000, greater than the number of transactions in Bitcoin network.

B. Block frequency

Second, we run experiments targeted at improving the consensus delay. For Bitcoin, it varies the frequency of block generation by reducing the proof-of-work difficulty.

In PBF, because each peer generates itself blocks and transactions. When a peer generates a peer block, this peer sends the peer block header to CP and VP set. The CP set generates key block by using Bitcoin hash function. So, in each peer, this is no consensus delay and the block frequency as faster as peer can. In Trusted-Trading network, construction peer competitively generates a key block, and validation peer validates the legality of key block by voting mechanism. After sending blocks, the peer can continue processing itself business. Figure 4 shows that the number of micro block per millisecond up to 10000. Figure 5 indicates that a key block just need one minutes to generate rather than ten minutes.

C. Block sizes

In Permissioned Blockchain Framework, for each block, block size dynamic change over time. In Bitcoin, large blocks take longer to verify and propagate. Therefore, although block frequency is constant, the time it takes for a miner to learn of a new block is longer. In PBF, it is not suitable that every peer has permission to generate key blocks. And, the content of every key block just contains a set of hash value, so the size of key block is very small, just a few KB, as shown in Figure 6. Figure 7 shows that the number of related transactions key block contains, which up to one hundred million.

II. CONCLUSION

In the past years, the lack of credibility has been becoming an urgent issue in various domains. Due to the inherent scalability barriers, Bitcoin-derived blockchains don't demonstrates better performance on E-commerce. This paper presents a Permissioned Blockchain Framework (PBF). The goal of PBF is to construct a higher credibility, lower latency E-commerce ecosystem. To improve the credibility of transactions, this paper presents a Permissioned Trusted Trading Network Consensus Algorithm (PTTNCA). The key idea of PTTNCA is to partition the network into sub-committees. To improve the throughput of transactions and consensus latency under a higher credibility, this paper presents a Peer Inner Blockchain Protocol (PIBP). PBF suggests better performance on throughput, latency, capacity in E-commerce.

In the future, we will do more work about the consensus algorithm, the storage mechanism of transactions and blocks, the no-sql retrieval mechanism of transactions.

ACKNOWLEDGMENT

This work is supported by National Natural Science Foundation of China under Grant No.61572295;Innovation Method Fund of China No.2015IM010200; the Natural Science Foundation of Shandong Province of China under Grant No.ZR2014FM031; Science and Technology Development Plan Project of Shandong Province No. 2014GGX101047, No.2015GGX101015; Shandong Province Independent Innovation Major Special Project No.2015ZDJQ01002, NO.2015ZDXX0201B03.

REFERENCES

[1] M. Swan. "Blockchain Thinking: The Brain as a DAC (Decentralized Autonomous Organization." In Texas Bitcoin Conference, pp. 27-29. 2015.

[2] M.Swan. "Blockchain: Blueprint for a New Economy." Sebastopol, CA: O'Reilly Media, 2015

[3] Blockchian.info, "Number of Transactions", [online]. Available: https://blockchain.info/charts/n-transactions.

[4] E.Sasson, A.Chiesa, C.Garman, M.Green, I.Miers, E.Tromer, M.Virza. "Zerocash: Decentralized anonymous payments from bitcoin". IEEE Security and Privacy (SP), pp459–474, 2014.

[5] A.Saxena, J.Misra, A.Dhar. "Increasing anonymity in bitcoin." Financial Cryptography and Data Security, Vol.8438, pp.122–139, 2014.

[6] I.Eyal, A.E.Gencer, E.G.Sirer, R.Renesse "Bitcoin-ng: A scalable blockchain protocol." 13th USENIX Symposium on Networked Systems Design and Implementation, NSDI, 2016

[7] M.Trent, M.Rodolphe, M.Andreas, D.Dimitri, M.Troy, M. Greg, H.Ryan, B.S, Y.Alberto. "BigchainDB: A Scalable Blockchain Database (DRAFT)." Technical report, 2016.

[8] A.Miller, J.Litton, A.Pachulski, N.Spring Neal Gupta, Dave Levin, Bobby Bhattacharjee. "Discovering Bitcoin's public topology and influential nodes." ACM Symposium on Applied Computing, pp.121-128. 2013

[9] D.Christian, R.Wattenhofer. "A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels". Stabilization, Safety, and Security of Distributed Systems. Vol. 9212, pp. 3–18, 2015.

[10] A.Miller, J. LaViola. Anonymous byzantine consensus from moderately-hard puzzles: A model for bitcoin. University of Central Florida. Tech Report, CS-TR-14-01, April 2014.

[11] A.Back, M.Corallo, L.Dashjr, M.Friedenbach, G.Maxwell, A.Miller, A.Poelstra, J.Tim′on, P.Wuille. "Enabling blockchain innovations with pegged sidechains." Technical Report. 2014. http://www.blockstream.com/sidechains.pdf.

[12] J.Garay, A.Kiayias, N.Leonardos. "The bitcoin backbone protocol: Analysis and applications." Advances in Cryptology-EUROCRYPT 2015. Springer Berlin Heidelberg, pp281-310, 2015.

[13] C.T. Li, Y. Yuan. "Block-chain based fragile watermarking scheme with superior localization." Optical Engineering, vol.5284, pp.147-160, 2008.

[14] L.Yoad, Y. Sompolinsky, A.ohar. "Inclusive block chain protocols." Financial Cryptography and Data Security, vol.8975, pp528-547. 2015.

[15] Heilman, Ethan, Foteini Baldimtsi, and Sharon Goldberg. "Blindly Signed Contracts: Anonymous On-Blockchain and Off-Blockchain Bitcoin Transactions." Fbim Transactions, pp37-48, 2015

[16] A.W.M. Dress, W. Wenzel, "Valuated matroid: A new look at the greedy algorithm", Applied Mathematics Letters, pp33-35, 1990.

[17] L.Ling. "A Fast Block-Greedy Algorithm for Quasi-optimal Meshless Trial Subspace Selection" SIAM Journal on Matrix Analysis and Applications, vol38. pp1224-1250 ,2016 .