E-commerce Blockchain Consensus Mechanism for Supporting High-Throughput and Real-Time Transaction

Yuqin Xu[1], Qingzhong Li[1,3(✉)], Xingpin Min[1], Lizhen Cui[1], Zongshui Xiao[2,3], and Lanju Kong[1]

[1] School of Computer Science and Technology, Shandong University, Jinan, China
xuyuqin_sdu@163.com, {Lqz,clz,klj}@sdu.edu.cn, minxingpin0105@163.com
[2] Electronic Commerce Research Center of Shandong University, Jinan, China
xzs@sdu.edu.cn
[3] Dareway Software Co., Ltd, Jinan, China

Abstract. Transactions may be altered, which leads to low credibility of transactions that restricts the rapid development and popularization of E-commerce. Although blockchain can ensure high stability and credibility of data, existing solutions still have some significant scalability barriers, such as low-throughput and high-latency. To improve credibility, this paper presents an e-commerce blockchain consensus mechanism (EBCM). EBCM does not rely on computing power and token but with the same level of security and credibility as Nakamoto consensus. Meanwhile, EBCM achieves real-time transaction and high-throughput. By introducing validation blockchain, we can ensure transactions cannot be altered. In order to realize high-throughput and real-time transaction, this paper constructs a two-layer blockchain. EBCM has been compared with Bitcoin in performance, and demonstrates better on throughput, latency.

Keywords: Credibility · Consensus mechanism · Blockchain scalability

1 Introduction

Shopping online which brings convenience to people's life is becoming more and more popular. So it is very important to build a secure and credibility e-commerce transaction network. Nowadays the lack of transactions' credibility is an urgent problem to be solved [1], because low credibility will seriously restrict the development of e-commerce. One possible method is to apply blockchain [2] to e-commerce, which can ensure high stability and credibility of data.

Consensus mechanism of Blockchain can solve the problem of trust and safety in distributed network. It is the key to building a safe and credible e-commerce transaction network, But existing blockchain mechanisms cannot support real-time transaction and high-throughput that e-commerce requires. In bitcoin [2], a transaction's confirmation time is an hour or so, that is fatal for e-commerce. Moreover, bitcoin's block size is not more than 1 MB, it only achieves a very small throughput [3]. So we propose an EBCM

S. Wang and A. Zhou (Eds.): CollaborateCom 2016, LNICST 201, pp. 490–496, 2017.
DOI: 10.1007/978-3-319-59288-6_46

which is suitable for e-commerce can help to build a safe, credible, public, autonomous e-commerce transaction network.

EBCM supports the similar blockchain data structure format as Bitcoin, we propose a modification that permits better efficiency. It guarantees credibility by introducing validation blockchain, and constructs a two-layer blockchain called peer blockchain to ensure high-throughput and real-time transaction. The contributions of our research are two-folds:

- We put forward EBCM which does not relay on computing power and token, but with the same level of security and credibility as Nakamoto consensus.
- EBCM can realize High-throughput, real-time transaction and no forks in blockchain.

The remainder of the paper is organized as follow: Sect. 2 introduces related work which had done lots of work for improving the performance of blockchain. In Sect. 3, we introduce an e-commerce transaction network. Section 4 describe consensus mechanism of creating blocks in detail. Section 5 introduces the experiment about EBCM.

2 Related Work

After POW [2], lots of researchers put forward some other mechanisms which can solve bad performance of blockchain. Sunny King proposed proof-of-stake (POS) [4], he thinks that blockchain should be created by those who have stakes. Although POS reduces transaction latency, it is far away from e-commerce requirement. Dan Larimer put forward Delegated Proof-of-Stake (DPOS) [5] which is similar to the voting mechanism of board, but it relies on tokens. Ittay Eyal presented Bitcoin-NG [3] which decouples Bitcoin's blockchain operation into two planes and divides time into epochs. Bitcoin-NG has better performance than bitcoin, and also relies on peer's computing power which does not apply to e-commerce. GHOST [6] introduced by Sompolinsky Y et al. modified the rule to accept the main valid blockchain in order to push more transactions to the network. But it requires higher bandwidths [7]. Loi Luu [8] designed SCP which can allow to reach consensus on blocks without broadcasting actual block data, while still enabling efficient block verification. But the performance of SCP are not enough for e-commerce.

3 E-commerce Transaction Network

In this section, we will introduce an e-commerce transaction network (BCTN) using EBCM based on p2p, which is showed in Fig. 1. BCTN integrates e-commerce trading center, which is convenient to the supervision department to audit. It composes of multiple peers and a Verification Network (VENT).

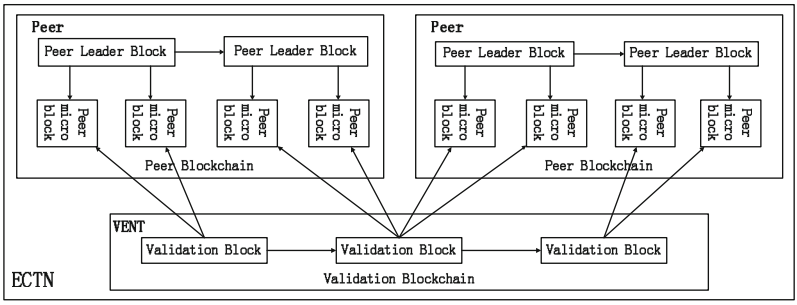

Fig. 1. E-commerce transaction network

Definition 1: Peer. A peer represents an e-commerce trading center or a logistics platform, such as Tmall. Each peer has an identity authentication, which can get public key for encrypting messages and private key for signing blocks. It can ensure the security of message and blocks cannot be forged.

Definition 2: Verification Network (VENT). Verification Network is composed of peers which has verification right, its function is to ensure that all peer micro blocks cannot be altered. Verification right means that the peer called verification peer (VP) has the right to construct validation blocks.

Peer blockchain designed as a two-layer blockchain ensures high-throughput and real-time transaction, it contains peer leader blocks and peer micro blocks. The structure of blocks are shown in Fig. 2. Peer micro block header contains: signature is used to identify the creator of the block, the GMT time is the creation time; the hash value of data is calculated transactions' hash by Sha256 algorithm which can ensure uniqueness and irreversibility. Peer leader block header includes all mentioned above, but with the hash value of previous block which can link peer leader block as blockchain.

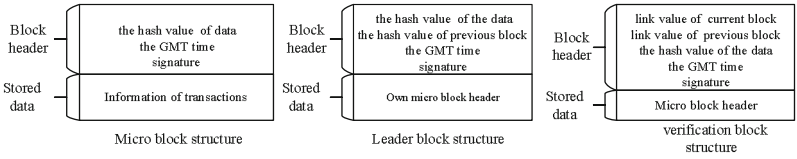

Fig. 2. Block structure

Validation blockchain shown in Fig. 2 stores all peer micro block headers to ensure that each peer micro block cannot be altered. The link value of current block and previous block can link all verification blocks into blockchain. How to calculate the link value will describe completely in Sect. 4.

The size of the micro block is fixed and the creation time is not greater than a predetermined value T_M, which can ensure real-time transaction. The number of block headers stored in peer leader block and verification block is also fixed value.

4 Consensus Mechanism of BCTN

In this section, we will describe EBCM in detail. In order to ensure EBCM has a same level of safe and credible, the process of creating blocks must promise that all blocks cannot be forged and altered.

4.1 The Creation Strategy of Peer Blockchain

We construct peer blockchain as two-layer blockchain to ensure high-throughput and real-time transactions. All transactions that saved in blocks are in chronological order. Peers cannot change transactions, cannot eliminate transactions, and cannot sort transactions artificially.

Each peer processes transactions which occur in it and verifies the legitimacy of transactions. After verification, transactions are temporarily stored in the memory pool. Transactions will be packaged into peer micro block until its size can satisfy or the time is more than T_M. After creating a complete peer micro block, the peer will send its header to all VPs in VENT and transactions store in the peer micro block can take effect. Multiple peer micro blocks can be created at the same time, which can realize high-throughput. Peers also need to create peer leader block as index which stored its own peer micro block headers. After calculating hash value of data and signing, the peer creates a complete peer leader block and then linked it to the leader blockchain. Peer leader block can be created only one at the same time.

4.2 Dynamic Verification Network

The process of creating verification block must be credibility to ensure peer micro blocks cannot be altered. We take two measures. Firstly, VPs in VENT is dynamically changed. Secondly, we propose a negotiated consensus algorithm which can promise that verification block cannot be forged as long as an honest peer existed in VENT.

This paper uses the credibility of peer (CRE), busy degree (B), computing power, and the number of times who had been as VP (T) to calculate peer's comprehensive value (C_V). Formula is as follows:

$$C\_V = \frac{CRE * (P/B)}{\sqrt{T}} \tag{1}$$

CRE is used to indicate the degree of peer's credibility, each peer's initial value is the same. And peer's CRE will reduce directly because of its malicious behavior. We use the number of peer micro blocks per hour to represent busy degree, its initial value is peer's average number of transactions per hour. To ensure VENT is dynamically changed, T is used as a limiting factor.

By using C_V, VENT sorts peers from big to small, the sequence is referred to as R_{C_V}. Assuming that the number of VPs in the verification network is N_V, and the VP set is constructed with peers which are in the top N_V of R_{C_V}.

4.3 Negotiated Consensus Algorithm

We propose a negotiated algorithm that does not rely on computing power, which can make sure the process of creating verification block is safe and credible.

First of all, all VPs reach a consensus on link value of validation block. Each VP in VENT creates a random number and signs, then sends it to other VPs. When a VP receives all VPs' random number, it can combine all VPs' random number as the link value. Considering information that may be lost or peer failure, we set two time thresholds T_{V1} and T_{V2} to prevent such situations. If the time that peer A waits for peer B's random number is more than T_{V1}, peer A requests peer B's random number to VENT. And If the time is more than T_{V2}, we will remove peer B from VENT. The remaining peers reach a consensus on the link value.

Secondly, VENT selects a VP to create a complete validation block by random numbers. A VP whose random number is the closest to the average of all random numbers and produces random number earlier, it will be selected. If other VPs do not receive validation block and the waiting time is more than T_D, the VP will lose the chance and the next VP gets the chance. After creating a complete validation block, the VP should send the feedback information to the peer whose micro block header has already been saved in it. The complete algorithm description of negotiated consensus is given in Algorithm 1.

Algorithm 1 Negotiated Consensus Algorithm

Input: the VP set
Output: validation block
1: Each peer creates a random number
2: Send random number with signature to other peers
3: **If** (the number of random numbers had been received = the number of VP -1)
4: block's link value = the sum of all the random number
5: **Jump to** step 16
6: **End if**
7: **Else if** (waiting time > T_{V1} && don't receive random number that send by Peer)
9: Send message for requesting random number
10: **Else if** (waiting time > T_{V2} && don't receive the Peer's random number
11: The Peer removed from the VP set
12: the number of VP = the number of CP -1
13: **End if**
14: Jump to step 3
15: **End if**
16: Average value = block's link value / the number of VP
17: Each peer's DIFF = Each peer's random number - Average value
18: Sort peer according to DIFF from small to large
16: **For**(i=1,i<= the number of VP, i++)
19: **If** (the rank of peer=i)
20: The peer is selected for creating block
21: **If**(the peer's response time >)
22: the CP lost creation right
23: **End If**
24: **End if**
25: **End for**
26: The Peer which is selected creates a complete block
27: Send to other Peers

Data consistency strategy for dynamic VP set. When a new VP set creates, if VENT just finishes creating a validation block, the new VP set will directly create the next validation block. Else, VENT will be forced to stop. For the micro block headers which have not been saved in validation block, the peer who sends them also do not receive the feedback information. So if peers once find VP set changed, then re-send peer micro block headers which do not have the feedback to VENT.

5 Experimental Evaluations

In this section, we evaluate EBCM with 1000-node experiments on an emulated network. The experiment implemented all EBCM elements that are significant. We take 2 s as a time slice, and the threshold value in the experiment is given in Table 1. We compare EBCM with Bitcoin in two sets of experiments, throughput and latency.

Table 1. The threshold value

Threshold	T_M	T_{V1}	T_{V2}	The size of micro block	The data entries of leader block and validation block	N_V
Value	2 s	5 s	10 s	1 MB	200	350

Figure 3 indicates the transaction latency of EBCM and bitcoin, EBCM is not more than 2 s that users can bear. Figure 4 shows throughput of transactions, EBCM can reach 100 thousands per second. The throughput of Tmall is about 120000 per second on November 11, 2015 which is the largest trading day of e-commerce in China. So we hold the opinion that EBCM can satisfy e-commerce requirement of performance. Through the statistical data we know the creation time of validation block is about 2 s, and the throughput of micro blocks can reach to 10000.

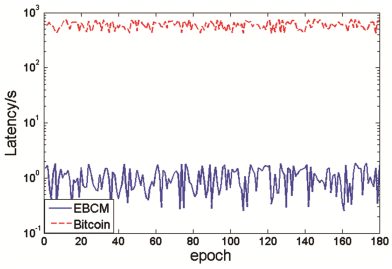

Fig. 3. Transaction latency

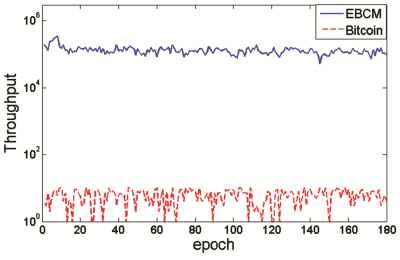

Fig. 4. Throughput of transactions

Through experiment, we can come to the conclusion that EBCM can satisfy the requirement of e-commerce. And under the same assumptions, EBCM has better performance than bitcoin.

6 Conclusion

This paper has been proposed EBCM which is suitable for e-commerce. EBCM can build a safe, credible, public, autonomous e-commerce transaction network to solve low credibility of transactions. It integrates e-commerce trading center as peer, which is convenient to the supervision department to carry out the audit. In the future, we will do more work about the storage mechanism of transactions and blocks, the no-sql retrieval mechanism, and a new mechanism to guarantee the data consistent.

Acknowledgment. This work is partially supported y SFC o.61572295; the Innovation Method Fund of China No. 2015IM010200; SDNSFC No.ZR2014FM031; the Science and Technology Development Plan Project of Shandong Province No. 2015GGX101015; the Shandong Province Independent Innovation Major Special Project No. 2015ZDXX0201B03.

References

1. Adelola, T., Dawson, R., et al.: Privacy and data protection in e-commerce in developing nations: evaluation of different data protection approaches (2015)
2. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. Consulted (2009)
3. Eyal, I., Gencer, A.E., Sirer, E.G., Renesse, R.V.: Bitcoin-NG: a scalable blockchain protocol (2015). http://arxiv.org/abs/1510.02037
4. King, S., Nadal, S.: PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake
5. Schuh, F., Larimer, D., BitShares 2.0: General Overview (2015)
6. Sompolinsky, Y., Zohar, A.: Secure high-rate transaction processing in bitcoin. In: Böhme, R., Okamoto, T. (eds.) FC 2015. LNCS, vol. 8975, pp. 507–527. Springer, Heidelberg (2015). doi: 10.1007/978-3-662-47854-7_32
7. Lewenberg, Y., Sompolinsky, Y., Zohar, A.: Inclusive block chain protocols. In: Böhme, R., Okamoto, T. (eds.) FC 2015. LNCS, vol. 8975, pp. 528–547. Springer, Heidelberg (2015). doi: 10.1007/978-3-662-47854-7_33
8. 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