A Novel Decentralized Blockchain Networks Model with High Concurrency*

*Blockchain Networks Model with High Concurrency

Linghao Zhang
State Gid Sichuan Electric Power Research Institute,
Chengdu 610000, China

Bingde Lu
State Gid Sichuan panzhihua Electric Power supply company
Panzhihua 617000, China

Tao Zhao
State Grid Big Data Center
Beijing 100031, China

Hongjun Wang
School of Information Science and Technology,
Southwest Jiaotong University
Chengdu 60031, China

***Abstract*—Blockchain is very important in finance field and electronic business field, so many researchers are attracted to study the technologies of blockchain. Since the transactions in blockchain takes much time, and they make the blockchain poor efficiency, business processes across organizations require the transactions as soon as possible. Concurrency is attracted much attention and is very important in blockchain field. In this paper, a novel decentralized blockchain network model with high concurrency is proposed. First, the idea of the proposed model is stated. Second, the high concurrency blockchain network model is proposed. Third, the corresponding algorithms are designed according to the proposed model. Furthermore, the experiment is conduced and the results show that proposed model works well.**

***Index Terms*—blokchain, decentralization blockchain, high concurrency, encrypted transaction**

I. Introduction

Blockchain is very popular in computer science field and finance field. There are so many researchers to study the technologies of blockchain, one of which is the concurrency in blockchain. The business activities of cross business organizations are beneficial to the organizations involved in the business, but it is difficult to trust each other within such business organizations [1]. In the Internet age, users need to be authenticated quickly, anonymously and efficiently [2]. In the process of supply chain management, all users of the supply chain need to effectively access customer demand, and track the demand realization process, carry out school teams for services, and realize the transparency of the supply chain [3]. Blockchain is a new technology for distributed transaction processing and data sharing in a large network composed of independent participants [4]–[8]. Blockchain-based approaches provide decentralized security and privacy [9]. It creates interesting research areas, mainly from the perspective of system self-organization and automatic operation [10].

This work is supported by the Blockchain Technology Fund of Hi-Tech Information Technology Research Institute of Chengdu (No. 2018H01207).

978-1-7281-2348-6/19/$31.00 ©2019 IEEE

More and more companies start offering digital payment systems [11]. For example, Nasdaq leveraged blockchain technology as part of an enterprise-wide initiative in 2015 [12]. The problem of maintaining complete control over and transparency with regard to our digital identity is growing more urgent as our lives become more dependent on online and digital services [13], [14]. In the era of e-commerce, the security and privacy of transaction information and user data information are a series of very challenging issues [15].

The distributed ledger technology (DLT) has been presented as potentially disruptive for financial market applications [16]. The public key infrastructure (PKI), which is commonly used now, is not perfect and has some security defects. Because it is the basis of security, more efforts are needed to improve PKI [17], [18]. Blockchain in the same domain authentication technology has been relatively mature, but in the process of cross domain authentication, there are still many problems. In order to solve the problem of cross domain authentication scheme of public key infrastructure (PKI), an effective cross domain authentication scheme with distributed multi center and collective maintenance is proposed. This scheme includes authentication protocol, Certificate Authorization Model and authentication architecture, which greatly improves the cross domain authentication protocol, security and efficiency [18].

Blockchains are also used for protecting software copyright [19], in Medical Field [20]–[22], cryptocurrency [23], [24], cross-border e-commerce between China and EU [25], the Internet of Things (IoT) scenario [26]–[28] and so on. According to the market rules, the cache strategy can be adjusted dynamically, mainly according to the market statistics obtained from the blockchain. However, for untrusted nodes, only the authenticity can be enforced financially through smart contract terms [29]. Although the cloud computing technology is changing more and more, it is more and more popular at the same time. However, the existing cloud storage technology also has shortcomings, lacking the support of corresponding execution rules, self-organizing contracts and data processing

requirements [30].

The rest of the paper is organized as follows. Related work is described in Section 2. In Section 3, we introduce the high concurrency blockchain network model and the corresponding algorithm is designed. In Section 4, experimental results are presented in detail. And the paper is concluded with further research topics in Section 5.

II. Related Work

In recent years, bitcoin system shows a new accounting mode, which shows the fairness of the system through everyone's accounting, and the self-organizing system runs well [14]. Since then, other projects demonstrated how these blockchains can serve other functions requiring trusted computing and suitability. The buzz surrounding Bitcoin [31]–[33] has reached a fever pitch [34] in 2015. A crucial ingredient into such systems is the "mining" of a Nakamoto blockchain [35]. The emergence of bitcoin in 2009 has aroused widespread concern, especially the development of cryptocurrency, which also provides a good case for the innovation of digital currency [36]. Cryptocurrency, within the reach of global network, shows the utility of participating in node consensus, which greatly changes the way of digital transaction [32]. In view of the shortcomings of bitcoin, the new blockchain protocol is designed to expand the existing scale of bitcoin. The new design of bitcoin trust model is better, more fault-tolerant and more robust, which avoids the qualitative change of digital currency ecosystem. [33].

Technological innovation can promote the development of digital infrastructure. At the same time, the reform of new social connection mode is also the driving force of digital infrastructure. [37]. Nakamoto's famous blockchain [38] protocol has a higher self-organization. As long as a consensus is reached, anyone can join in the implementation of the protocol, and can also leave the blockchain according to the protocol. Recdactable [39] is a new relatively free blockchain framework, which does not solidify the content quantity of each block, but also allows the block content to be rewritten in the decentralized service. Ouroboros [40] is a very strict blockchain protocol, which can seriously guarantee the security of users and prove that the protocol is very secure. ProvChain [41] is a kind of block chain architecture to enhance privacy, and this architecture runs in the cloud environment, which can manage data well. Solida [42]is an extension of Byzantine consensus protocol, which is proved to be a decentralized blockchain protocol through work. ForkBase [43] is a storage engine, which divides the blockchain management by protocol, integrates the core applications and provides interfaces for other developers, which can reduce workload and improve work efficiency. An article discusses the organization of social sharing. Good social sharing may be achieved through the development of blockchain technology. At the same time, through research, blockchain technology has this strength [44]. Some scientists think that at present, blocks are relatively scattered, and each block is linked to each other to form a large, transparent, safe, reliable and timely system [45].

Ethereum blockchain [5] is the development of blockchain technology. Users can use it to build smart contracts that are recognized by everyone, which can be implemented programmatically. In this way, Ethereum can not only carry the function of digital currency, but also a network that can execute smart contracts. As is known, if the transaction is sent and executed twice, and executed serially by the block, the transaction efficiency will be closely related to the number of trading users. This will reduce the overall transaction efficiency. The block chain which supports for highly concurrent decentralized trusted computing networks is an important research in encrypted account transaction chain. Although reliability enhancement and various fault tolerance techniques have been widely studied in block chain, changing the serial execution of the block to concurrent execution brings new challenge to the research.

To overcome these challenges and realize encrypted account transaction chain, we proposed a high concurrency blockchain chain technology and have done some particular works to realize the computing network:

1) Try to remove the block, so that the transaction is not sent and executed twice.
2) Change the serial execution of the block to the concurrent execution of the unlimited number of transactions (in number of user accounts).
3) Transaction efficiency has nothing to do with the number of trading users, but only depends on the communication delay of the network and the computing power of the CPU.

III. High concurrency blockchain network model

A. Basic Idea

Blockchain is a self-organizing system, which organizes a distributed network through P2P protocol and participates in self-organizing work through each node. First, when there is a transaction in the blockchain system, the transaction details are represented by numbers, and the package code mapping becomes a unique indicator. Secondly, each block is linked according to the serial number, and it is neither changeable nor reversible, forming a serial data chain, which can prevent the block change and the orderly chain from being blocked. This data chain is a blockchain, which is actually a shared recording system, recording the facts and transactions of the block, and each member can access and participate in the verification. The verified block will be permanently recorded, and no one can delete it.

The state library and the current Ethereum state library remain unchanged, and the structure is: (1)Account;(2)Status of the account.The status of the account includes the balance of the account; for the contract account, the code of execution and related storage are included. The encrypted account transaction chain consists of several parts:(1) Encrypted account prime list, structured as: account, latest transaction number of the

account;(2) Encrypted account chain, structured as: account transaction number, transaction. World status of the account equals encrypted account transaction chain acts on the state transfer function. It can be calculated by the following equation:

$$S(t) = F(C(t)) \tag{1}$$

where $S(t)$ is the structure, $C(t)$ is account transaction number related the corresponding transaction, and F is hash function. Structure of the transaction is designed to add an item to the data structure of the existing transaction, the transaction parent hash, used to store the hash of the previous transaction for the account corresponding to the transaction.

$$T(i).ParentHash = T(i-1).Hash \tag{2}$$

where T is transaction.

B. High Concurrency Blockchain Network Algorithms

In this subsection, High concurrency blockchain network model(HCBNM) mainly includes two algorithms, and they are illustrated in detail. One is transaction issuing and broadcasting process algorithm as Algorithm 1 shows, the other is Synchronous process algorithm as Algorithm 2 shows.

Algorithm 1: transaction issuing and broadcasting process

1) The account owner issues a transaction and signs it;
2) The transaction first updates the encrypted account index table of the node, encrypts the account chain, and executes the transaction update status library;
3) Broadcasting a new transaction to the P2P related node;
4) After receiving the new transaction information, the relevant P2P node uses the local encrypted account index table, the encrypted account chain and the relevant compliance rules of the transaction to verify the transaction;
5) The transaction verification is passed, the encrypted account index table of the node where the node is located, the encrypted account chain, and the transaction update state library are executed;
6) Broadcast the transaction to other nodes of the node.

The synchronous process is for the time when the nodes are newly created or cannot be synchronized with the network due to downtime.

Algorithm 2: Synchronous process

1) Sending a request to the peer-to-peer(P2P) node to obtain an encrypted account index table;
2) Using the retrieved encrypted account index table, compare with the local encrypted account index table to obtain a list of transactions that need to be synchronized;
3) Requesting transaction synchronization from the P2P node according to the transaction list to be synchronized;
4) The relevant P2P node sends the requested transaction to the synchronization requesting node;
5) After requesting the transaction, the transaction is verified for compliance. For the transaction that meets the requirements, the transaction index table, the encrypted account chain are updated, and the transaction pool is placed in time series;
6) If the synchronization has been completed, execute the transaction in the trading pool and update the status library.

The two algorithms work together to combine HCBNM, and they can ensure that concurrency in blockchain is enhanced.

IV. Experiments

A. Experimental Setup

In this subsection, the experimental steps are illustrated and experimental results are reported in detail.

Geth is used to develop a private blockchain system in our local area network This system is mainly to simulate the high efficiency of transactions. Therefore, in the experiment, the difficulty of hash algorithm is not considered, or it can be realized by simple hash algorithm. The whole experimental system is realized by go language.

B. Distributed Execution Implementation

The basic situation of the experimental setup is that six clients form a self-organizing network, the client monitoring system has a verified transaction amount, and then the client sends the transaction. Then wait for the last transaction T^{-1} to commit before starting the current transactionT^0.

The distributed execution is as follows:

1. Choose to setup geth online as an Ubuntu user and run the following codes.

2. Check whether the geth was setup successfully.

```
copy@ubuntu: $ geth help
```

3. Establish private Ethereum network.

```
copy@ubuntu: $ mkdir private-geth
copy@ubuntu: $ cd private-geth/
```

4. Write the block content in a file. Prepare the creation block and execute the initialization command.

5. Create a new account and start mining.

```
> personal.newAccount( "123") "0x04db853fe43494022f7f961091c1764709aa5f87"
> miner.start()
```

C. Experimental Results

As the speed of the block appearance would be an important index to evaluate the efficiency of the transaction, we are going to use the speed of the emergence of blocks to represent the fastest speed of the transaction. Sum-of-concurrency (SOC) is used to measure the number of the concurrency in the system with respect to the same situation. The sum-of-concurrency (SOC) is defined as $SOC = \sum_{i=1}^{k} a_i$, where k is the number of nodes, and a_i denotes the number of concurrency in the

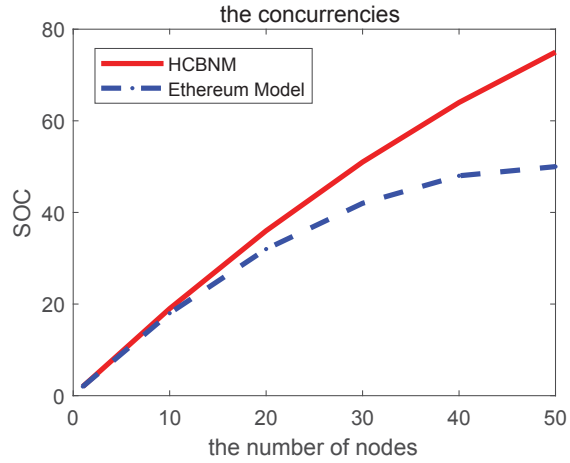

Fig. 1. Concurrency results are in the two models, and higher is better.

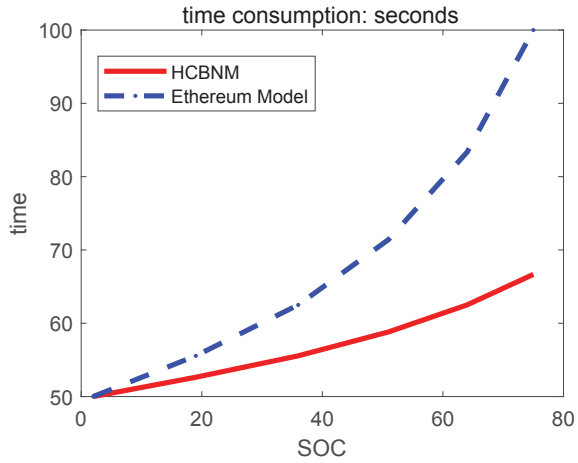

Fig. 2. Time-consumption results are in the two models, and lower is better.

node i that processes the task. The higher SOC, and the better performance.

The result is reported in Fig 1. The x-axis represents the number of nodes, and the y-axis shows the corresponding SOC value for each number of nodes. It is clearly that the proposed model outperforms the Ethereum model and obtains the best SOC result.

Furthermore, the same concurrency is used to test the time consumption and the result is recorded as Fig 2 shows. The x-axis represents sum-of-concurrency, and the y-axis shows the corresponding time-consumption value. It is clearly that the proposed model need less time than the Ethereum model, which shows that the proposed model obtains better performance.

In this experiment, the transaction efficiency has nothing to do with the number of trading users on the basis of the third generation of blockchain technology, but only depends on the communication delay of the network and the computing power of the CPU. What's more, the decentralized and trusted computing networks is a good characteristic of the third generation of blockchain technology. Blockchain technology plays a vital role in decentralized trusted transactions, and this experiment shows its high speed and rapidity.

V. Conclusions

In this paper, a novel decentralized blockchain network model with high concurrency is proposed, and its idea of the proposed model is stated. According the idea, high concurrency blockchain network model is illustrated in detail, and it includes two algorithms: One is transaction issuing and broadcasting process algorithm, the other is Synchronous process algorithm. At last, the model is implemented to test its performance, and two evaluation standards of SOC and time-consumption are used for the experiments, and the results show that proposed model works well. Even though the proposed model enhances the concurrency, and in the future, concurrency is also am important research problem among blockchain field. We will focus on the protocol to speed the concurrency of blockchain.

References

[1] I. Weber, X. Xu, R. Riveret, G. Governatori, A. Ponomarev, J. Mendling, Untrusted business process monitoring and execution using blockchain, in: International Conference on Business Process Management, 2016, pp. 329–347.
[2] G. W. Peters, E. Panayi, A. Chapelle, Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective, Vol. 3, 2013.
[3] K. Korpela, J. Hallikas, T. Dahlberg, Digital supply chain transformation toward blockchain integration, in: Hawaii International Conference on System Sciences, 2017.
[4] X. Xu, C. Pautasso, L. Zhu, V. Gramoli, A. Ponomarev, B. T. An, S. Chen, The blockchain as a software connector, in: Software Architecture, 2016, pp. 182–191.
[5] R. Beck, J. S. Czepluch, N. Lollike, S. Malone, Blockchain c the gateway to trust-free cryptographic transactions, in: Twenty-Fourth European Conference on Information Systems, 2016.
[6] A. Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou, Hawk: The blockchain model of cryptography and privacy-preserving smart contracts, in: Security and Privacy, 2016, pp. 839–858.
[7] X. Cai, Development of localized cloud computing big data application based on blockchain technology, 2018.
[8] J. Kishigami, S. Fujimura, H. Watanabe, A. Nakadaira, A. Akutsu, The blockchain-based digital content distribution system, in: IEEE Fifth International Conference on Big Data and Cloud Computing, 2015, pp. 187–190.
[9] A. Dorri, S. S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for iot security and privacy: The case study of a smart home, in: IEEE International Conference on Pervasive Computing and Communications Workshops, 2017.
[10] J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander, Where is current research on blockchain technology?-a systematic review, Vol. 11, 2016, p. e0163477.
[11] S. Trimborn, W. K. H?rdle, Crix or evaluating blockchain based currencies, 2015.
[12] J. D'Antona, Nasdaq launches enterprise-wide blockchain technology initiative, 2015.
[13] A. Lazarovich, Invisible ink : blockchain for data privacy, 2015.
[14] G. Zyskind, O. Nathan, Alex, Decentralizing privacy: Using blockchain to protect personal data, in: IEEE Security and Privacy Workshops, 2015, pp. 180–184.
[15] N. Z. Aitzhan, D. Svetinovic, Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams, Vol. PP, 2016, pp. 1–1.
[16] F. M. Ametrano, Bitcoin, blockchain, and distributed ledger technology, 2016.

[17] L. Axon, Privacy-awareness in blockchain-based pki, 2015.
[18] Z. Zhou, L. I. Lixin, L. I. Zuohui, Efficient cross-domain authentication scheme based on blockchain technology, 2018.
[19] J. Herbert, A. Litchfield, A novel method for decentralised peer-to-peer software license validation using cryptocurrency blockchain technology, in: Australasian Computer Science Conference, 2015.
[20] X. Yue, H. Wang, D. Jin, M. Li, W. Jiang, Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control., Journal of Medical Systems 40 (10) (2016) 218.
[21] N. I. Pei-Kun, S. O. Business, Q. University, Study on value of blockchain technology in medical field, 2018.
[22] R. Mezaromero, G. Benedek, X. Yu, J. L. Mooney, R. Dahan, N. Duvshani, R. Bucala, H. Offner, Y. Reiter, G. G. Burrows, Hla-dr1 constructs block cd74 expression and mif effects in experimental autoimmune encephalomyelitis., Vol. 192, 2014, pp. 4164–73.
[23] Z. He, X. Li, L. Zhan, Z. Wu, D. O. Automation, Data integrity protection method for microorganism sampling robots based on blockchain technology, 2015.
[24] I. Ahmed, A. James, D. Singh, Critical analysis of counter mode with cipher block chain message authentication mode protocolłccmp, Vol. 7, 2014, pp. 293–308.
[25] Y. B. Zhang, The new ecosystem of cross-border e-commerce between eu and china based on blockchain, 2018.
[26] M. Conoscenti, A. Vetr, J. C. D. Martin, Blockchain for the internet of things: A systematic literature review, in: Computer Systems and Applications, 2017.
[27] A. Ouaddah, A. A. Elkalam, A. A. Ouahman, Towards a novel privacy-preserving access control model based on blockchain technology in iot, 2017.
[28] N. Kshetri, Can blockchain strengthen the internet of things?, Vol. 19, 2017, pp. 68–72.
[29] W. Wang, D. Niyato, P. Wang, A. Leshem, Decentralized caching for content delivery based on blockchain: A game theoretic perspective, 2018.
[30] R. Matzutt, J. Hiller, M. Henze, J. H. Ziegeldorf, D. Mllmann, O. Hohlfeld, K. Wehrle, A quantitative analysis of the impact of arbitrary blockchain content on bitcoin, in: Financial Cryptography and Data Security, 2018.
[31] H. B. Shadab, Regulating bitcoin and block chain derivatives, 2014.
[32] M. Vukoli?, The quest for scalable blockchain fabric: Proof-of-work vs. bft replication, in: International Workshop on Open Problems in Network Security, 2015, pp. 112–125.
[33] I. Eyal, A. E. Gencer, R. V. Renesse, Bitcoin-ng: a scalable blockchain protocol, in: Usenix Conference on Networked Systems Design and Implementation, 2016, pp. 45–59.
[34] T. I. Kiviat, Beyond bitcoin: Issues in regulating blockchain transactions, Vol. 65, 2015.
[35] D. Kraft, Difficulty control for blockchain-based consensus systems, Peer-to-Peer Networking and Applications 9 (2) (2016) 397–413.
[36] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell, A. Miller, A. Poelstra, J. Timn, P. Wuille, Enabling blockchain innovations with pegged sidechains, 2014.
[37] F. Glaser, Pervasive decentralisation of digital infrastructures: A framework for blockchain enabled system and use case analysis, 2017.
[38] R. Pass, L. Seeman, A. Shelat, Analysis of the blockchain protocol in asynchronous networks, 2017.
[39] G. Ateniese, B. Magri, D. Venturi, E. Andrade, Redactable blockchain c or c rewriting history in bitcoin and friends, in: IEEE European Symposium on Security and Privacy, 2017, pp. 111–126.
[40] A. Kiayias, A. Russell, B. David, R. Oliynykov, Ouroboros: A provably secure proof-of-stake blockchain protocol, in: International Cryptology Conference, 2017, pp. 357–388.
[41] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, L. Njilla, Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability, in: Ieee/acm International Symposium on Cluster, Cloud and Grid Computing, 2017, pp. 468–477.
[42] I. Abraham, D. Malkhi, K. Nayak, L. Ren, A. Spiegelman, Solida: A blockchain protocol based on reconfigurable byzantine consensus, 2018.
[43] S. Wang, T. T. A. Dinh, Q. Lin, Z. Xie, M. Zhang, Q. Cai, G. Chen, W. Fu, B. C. Ooi, P. Ruan, Forkbase: An efficient storage engine for blockchain and forkable applications, 2018.
[44] A. Pazaitis, P. De Filippi, V. Kostakis, Blockchain and value systems in the sharing economy: The illustrative case of backfeed, Vol. 125, 2018.
[45] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie, M. Bertoncini, Blockchain based decentralized management of demand response programs in smart energy grids, Sensors 18 (1) (2018) 162.