A Novel Decentralized Blockchain Networks Model with High Concurrency

Yimiao Zhao[1]and Linghao Zhang[2], Bingde Lu[3], Tao Zhang[3], Qigang Zhao[1], and Hongjun Wang[1]

[1] School of Information Science and Technology, Southwest Jiaotong University, Chengdu 60031, China
714453081@qq.com
[2] State Gid Sichuan Electric Power Research Institute, Chengdu 610000, China
[3] State Gid Sichuan panzhihua Electric Power supply company, Panzhihua 617000, China

Abstract. Concurrency is attracted much attention in blockchain field. In this paper, we propose a novel decentralized blockchain network model with high concurrency. First, the idea of the proposed model is stated. Second, the high concurrency blockchain network model is proposed. Third, the corresponding algorithm is designed according to the proposed model. Furthermore, the experiment is conduced and the results show that proposed model works well.

Keywords: Blokchain · Decentralization blockchain · High concurrency · Encrypted transaction

1 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 integration of business processes across organizations is typically beneficial for all involved parties. However, the lack of trust is often a roadblock[1]. The internet era has generated a requirement for low cost, anonymous and rapidly verifiable transactions to be used for online barter[2]. Access to customer demand needs to be shared effectively, and product and service deliveries must be tracked to provide visibility in the supply chain[3]. Blockchain is an emerging technology for decentralized and transactional data sharing across a large network of untrusted participants[4–8]. Blockchain-based approaches provide decentralized security and privacy[9]. It creates interesting research areas, especially from the perspective of technical challenges and limitations[10].

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]. The issues

related to the security and privacy of consumption and trading data present serious challenges[15].

The distributed ledger technology (DLT) has been presented as potentially disruptive for financial market applications[16]. Conventional public key infrastructure (PKI) designs are not optimal and contain security flaws; there is much work underway in improving PKI[17, 18]. To solve the efficiency problem of the existing Public Key Infrastructure(PKI) cross-domain authentication scheme, by using blockchain technology with the advantages of distributed multi-center, collective maintenance and not being easy to tamper, an effective cross-domain authentication scheme was proposed, including Block Chain Certificate Authority(BCCA) trust model and system architecture, blockchain certificate format and user cross-domain authentication protocol, as well as the 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. In the market, the cache helpers are able to autonomously adapt their caching strategies according to the market statistics obtained from the block chain, and the truthfulness of trustless nodes are financially enforced by smart contract terms[29]. Despite their increasing proliferation and technical variety, existing cloud storage technologies by design lack support for enforcing compliance with regulatory, organizational, or contractual data handling requirements[30].

The rest of the paper is organized as follows. We describe related work 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. Finally, the paper ends with conclusions and further research topics in Section 5.

2 Related work

In recent years, a new class of accountable systems emerged. The first such system was Bitcoin[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]. Since the introduction of Bitcoin[Nak09] in 2009, and the multiple computer science and electronic cash innovations it brought. There has been great interest in the potential of decentralised cryptocurrencies[36]. Bitcoin cryptocurrency demonstrated the utility of global consensus across thousands of nodes, changing the world of digital transactions forever[32]. Bitcoin-NG, a new blockchain protocol designed to scale. Based on Bitcoin's blockchain protocol, Bitcoin-NG is Byzantine fault tolerant, is robust to extreme churn, and shares the same trust model obviating qualitative changes to the ecosystem[33].

Technological innovation and consequential decentralisation are driving forces in the ongoing evolution and increasing openness of digital infrastructures [37].

Nakamotos famous blockchain[38] protocol enables achieving consensus in a so-called permissionless settinganyone can join (or leave) the protocol execution. Recdactable blockchain[39] is a new framework that makes it possible to re-write or compress the content of any number of blocks in decentralized services exploiting the blockchain technology. Ouroboros[40] is the first blockchain protocol based on proof of stake with rigorous security guarantees. ProvChain[41] is a blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability. Solida[42], a decentralized blockchain protocol based on reconfigurable Byzantine consensus augmented by proof-of-work. ForkBase[43], a storage engine specifically designed to provide efficient support for blockchain and forkable applications.By integrating the core application properties into the storage, ForkBase not only delivers high performance but also reduces development effort.An article explores the potential of blockchain technology in enabling a new system of value that will better support the dynamics of social sharing[44]. Some scientists investigated the use of decentralized blockchain mechanisms for delivering transparent, secure, reliable, and timely energy flexibility[45].

The Ethereum blockchain[5] allows user-created digital smart contracts to be executed by implementing a generically programmable code. It is not solely a net work for exchanging cryptocurrencies but a network where transactions can be used to execute an unlimited number of self-developed 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.

3 High concurrency blockchain network model

3.1 Basic idea

Blockchain is a distributed network and it works on its own way. First of all, as each transaction occurs - and the parties agree to its details - its encoded into

a block of digital data and uniquely signed or identified. Secondly, each block is connected to the one before and after it - creating an irreversible, immutable chain. And then, blocks are chained together, preventing any block from being altered or a block being inserted between two existing blocks. Blockchain creates a shared system of record among business network members, eliminating the need to reconcile disparate ledgers. And then, its permissioned.Each member of the network must have access privileges. Information is shared only on a need-to-know basis. Last but not the least, its immutable. Consensus is required from all members and all validated transactions are permanently recorded. Even a system administrator cant delete a transaction.

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:

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

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.

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

3.2 High concurrency blockchain network Algorithms

In this subsection, the algorithms of high concurrency blockchain network are illustrated in detail. It includes two steps: one is transaction issuing and broadcasting process, the other is Synchronous process.

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 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.

3.3 Motivation and network security protection

In this subsection, we will first introduce the method of motivation and network security protection, which is fuel and mining mechanisms. The goal is to ensure network security and avoid abuse of transactions by user accounts, thus using a fuel mechanism; The incentive node builds a synchronization node and participates in the storage and data services of the public book.

Gas mechanism. One of the more important concepts in Ethereum is the fees, which are incurred for every calculation generated by transactions on the Ethereum networkno free lunch. This fee is paid for what is called "gas".

Gas is used to measure the cost units required in a specific calculation. Gas price is the amount you want to spend Ether on each gas, measured by "gwei". "Wei" is the smallest unit of Ether, 1 Ether means 10^{18} Wei. 1 gwei is 1,000,000,000 Wei.

For each transaction, the sender sets the gas limit and gas price. The gas limit and the gas price represent the maximum value of the Wei that the sender

is willing to pay for the execution of the transaction. For example, suppose the sender sets the gas limit to 50,000 and the gas price to 20 gwei. This means that the sender is willing to pay up to 50,000*20 gwei = 1,000,000,000,000,000 Wei = 0.001 Ether to execute this transaction.

The gas limit represents the maximum amount of money the user is willing to spend on the gas. If there is enough Ether in their account balance to pay for this maximum cost, then there is no problem. Any unused gas at the end of the transaction will be returned to the sender for redemption at the original rate. If the sender does not provide enough gas to execute the transaction, then the trade execution will appear "gas is insufficient" and then considered invalid. In this case, the transaction processing will be terminated and all changed states will be restored, and finally we will return to the state before the transaction - the state before the completeness is like this transaction never happened. Because the machine is still working on calculations before running out of gas, in theory, no gas will be returned to the sender.

Where did the money for these gas go? All the money the sender spends on the gas is sent to the "beneficiary" address, which is usually the address of the miner. Because the miners made an effort to calculate and verify the transaction, the miner received the cost of the gas as a reward.

Usually, the sender is willing to pay a higher gas price, and the miner will always get more value from the deal. Therefore, the miners are more willing to choose this deal. In this case, the miner is free to choose a transaction that he is willing to verify or ignore. In order to guide the sender to set the gas price, the miner can choose to suggest a minimum gas value and they are willing to execute a trade.

This mechanism follows the following principles:

(1) Each account calculates the gas fee based on the fuel price in the network before sending the transaction;

(2) The user sends a transaction, and when each node executes the transaction, the gas fee and the transfer amount will be deducted from the account balance, and the gas fee is paid to the mining public account;

(3) In order to prevent double spending, the transaction must be executed serially according to the transaction sequence number of the account; when the transaction is synchronized, all transactions are executed serially according to the transaction timing and transaction sequence number.

Mining mechanism. In order for a state to be converted to the next state, the transaction must be valid. In order for a transaction to be considered valid, it must go through a verification process, which is mining. Mining is a group of nodes (ie computers) that use their computing resources to create a block containing valid transactions.

Any node that claims to be a miner on the network can try to create and verify blocks. Many miners around the world create and validate blocks at the same time. Each miner provides a "proof" of the mathematical mechanism when

submitting a block to the blockchain. This proof is like a guarantee: if the proof exists, then the block must be valid.

In order for a block to be added to the main chain, a miner must provide this "proof" faster than other miners. The process of confirming each block by the "proof" of a mathematical mechanism provided by the miner is called the proof of the work.

This mechanism follows the following principles:

(1) Encrypted account transaction chain sets up a public contract account, stores the mining funds preset by the system, adopts a daily fixed-distribution mechanism, and halve the issuance at the agreed time, which is infinitely zero;

(2) Use the mining account weight based on the contract account to allocate the daily mining transaction fee and the daily mining fund issued by the system.

4 Experiments

4.1 Experimental setup

We deployed a private blockchain system in our local area network using geth version 1.4.0, which is a Go implementation of the command line interface for running an Ethereum node. We setup three machine connected through a 1 Gbps network, two consisting of miners, p1 and p3, generating blocks and on consisting of a peer p2 simply submitting transactions.

We artificially reduce the difficulty of the hash algorithm in order to observe and record the speed of the emergence of blocks. 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.

In order to record the mining process and the out velocity on different platforms, we also use an application called 'Wacoin' to simulate the mining process.

4.2 Distributed execution

In our experiment, the client only sends coins once the peer owns a verified amount of coins. The peer performs a transaction t2 only if it was shown by the system that the previous transaction t1 had been committed and the money was successfully transferred to its wallet.

The distributed execution is as follows:

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

```
$ sudo add-apt-repository -y ppa:ethereum/ethereum
$ sudo apt-get update
$ sudo apt-get install ethereum
```

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 following content in a file called 'genesis.json'. Prepare the creation block and execute the initialization command.

```
root@ubuntu:/home/ubuntu/private-geth
{
"config": {
"chainId": 15,
"homesteadBlock": 0,
"eip155Block": 0,
"eip158Block": 0
}
"coinbase" : "0x0000000000000000000000000000000000000000",
"difficulty" : "0x40000",
"extraData" : "",
"gasLimit" : "0xffffffff",
"nonce" : "0x0000000000000042",
"mixhash" : "0x0000000000000000000000000000000000000000000000000000000000000000",
"parentHash" : "0x0000000000000000000000000000000000000000000000000000000000000000",
"timestamp" : "0x00",
"alloc": { }
}
root@ubuntu:/home/ubuntu/private-geth
```

5. Create a new account and start mining.

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

4.3 Analysis of experimental results

We record the speed of mining of the blockchain in the private blockchain system in our local area network.

The experimental results show that the speed of the block appearance is about 465.775μs, which means that the blockchain support for high-efficiency transaction. 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.

5 Conclusions

In this paper, we examine the problem of blockchain transaction reliability enhancement. In our proposed approach, if the block is removed, the transaction would not be sent and executed twice. This makes the trading easier and faster. What's more, if we change the serial execution of the block to the concurrent execution of the unlimited number of transactions (in number of user accounts), it would improves the overall efficiency of the transaction. We raise the model that the 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, in which way the stability of the transaction is not vulnerable to external changes.

Our future work will involve realizing and enhancing the reliability and of the third generation of blockchain technology. We will also consider how provide more efficient and stable trading methods for blockchains.

6 References

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 protocolccmp, 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.