Research Summary of Blockchain Fragmentation Propagation Mechanism Based on Merkel Tree

Tian Liwei¹, Sun Yu²
¹Guangdong University of science and technology, Dong guan, 523083, China
²Guangdong University of Technology, Guang zhou, 510006, China

Email: 656453927@qq.com

Abstract. At present, when the blockchain system propagates blocks, it is a point-to-point propagation of complete blocks. This method has three shortcomings: the propagation load is large; the message can only be received from one node; only after the complete block is received, can it be propagated to other nodes. Therefore, this article considers changing the block's Merkel tree data structure to minimize the data size during block propagation while ensuring that the receiving node can reconstruct the correct and complete block. On the other hand, in order to be able to receive blocks from multiple nodes at the same time and relay to other nodes when incompletely received, the blocks are fragmented and then reorganized. At the same time, the correctness of a single fragment can also be verified.

Key words. Blockchain, Merkel tree, Shard propagation

1. Introduction
Blockchain is the core of Bitcoin. It uses peer-to-peer network communication to back up transaction data at every node in the system, thereby building a huge distributed public account book. Due to the asynchronous nature of the network, mining competition, and BGP routing hijacking, the Bitcoin blockchain may fork. Forking will destroy the consistency of data between nodes and affect the security and availability of the system. In the case of a fork, only a few intermediate nodes can detect the existence of the fork, and most of the unknowing nodes will continue to mine on their respective chains. For the entire network, the computing power of nodes is actually fragmented, which will directly reduce the rate of block generation and affect system performance. The synchronization efficiency of blocks is related to the security and usability of the entire system. It is a factor that must be fully considered when designing and applying blockchain technology, and it is a very important research object.

In addition, the network composed of all Bitcoin nodes is a fully distributed topology, and the transmission process between nodes is closer to the "flooding algorithm", that is: transactions are generated from a node and then broadcast to the neighboring node, the neighboring node will be transmitted to ten, ten to a hundred, until it spreads to the entire network. The purely distributed structure does not have the single-point performance bottleneck and single-point failure problems of the centralized structure, and has good scalability, but the flooding mechanism introduces new problems, mainly the problem of poor controllability, and the core problem The network transmission load caused by flooding is relatively large, so it is of great practical significance to design a mechanism to reduce the Bitcoin network transmission load.

2. Research status
2.1. Block propagation in the blockchain system
Recently, a large number of scholars are committed to using clustering methods to reduce the number of routing hops in block propagation to reduce propagation delay. In [1], the author proposed the blockchain system clustering protocol BCBSN based on super nodes, which can cluster nodes according to the local characteristics of nodes in the blockchain system, and by specifying one in each cluster, the central node connects the remaining nodes in this category with the central node, thereby reducing the number of routing hops required for network propagation. As the number of routing hops decreases, the propagation delay will also decrease. Subsequently in [2], the author evaluated the BCBSN protocol, which further proved its effectiveness in improving the block propagation speed. In [3], the author proposed a BCBPT protocol that clusters nodes based on the Ping delay between nodes to reduce the propagation delay of adjacent nodes in the network. Depending on the geographical location of the adjacent nodes in the network, there may be changes between each other. The principle of multiple hops uses the delay generated by the Ping command to measure the network distance between nodes, so as to avoid spreading blocks to geographically adjacent nodes.

2.2. The increase of blockchain transaction throughput
In [4], the author proposed the Bitcoin-NG protocol, introducing two different blocks: key blocks for electing leaders and micro blocks containing transaction data. The generation of key blocks is similar to the traditional Bitcoin mining process. Once a node successfully mines, the generated key block will be propagated to other nodes, thus becoming a temporary leader. After the leader confirms, multiple micro-blocks will be generated within a certain period of time. The author believes that through such a mechanism, not only can the expansion problem in Bitcoin be solved, but also the delay in verifying transactions can be reduced. In [5], the author proposed Algorand based on Verifiable Random Function (VRF) [6] and the BA protocol. According to the property (PoS) owned by the node, it forms a committee through a lottery mechanism, and then runs the BA protocol in the committee to generate the next new block. The number of transactions confirmed in one minute is 125 times that of Bitcoin, which greatly expands the throughput of the blockchain. However, when the PoS consensus system is forked, nodes can mine on multiple chains at the same time without losing any resources, and finally obtain all the benefits, resulting in the "nothing at stake" problem.

2.3. Application of Sharding Technology in Blockchain System
Elastico [7] applied the design principles of the fragmentation technology used in the database system to fragment the network to improve transaction throughput. Monoxide[8] is also one of the blockchain designs that apply sharding technology. The main difference from Elastico is that Monoxide not only shards the nodes through proof of work to form multiple committees, but also shards the blockchain. Each committee maintains a blockchain shard, and the new blocks generated will only be stored in the committee to which it belongs. In short, Monoxide improves transaction throughput and reduces the cost of nodes storing blockchain information.

2.4. Blockchain security
Sabre [9] is a secure and scalable Bitcoin relay network that can mitigate existing BGP hijacking attacks to a certain extent [10]. It proposes to arrange a set of Sabre relay nodes in the Bitcoin network to connect each Bitcoin node to resist BGP routing hijacking. But it also increases the network communication overhead, which reduces the transaction throughput.

2.5. Network coding (in P2P network)
Experiments in [11] show that network coding is practical in P2P networks. It has a small overhead in CPU processing and I/O, which can make network downloads fast and efficiently use server resources. It actually applies the network coding theory to the P2P message distribution mechanism, which enables nodes to integrate and compress the bit streams transmitted in the network through algorithms, so that the network content distribution mechanism has the following characteristics: quickly locate resources;
accelerate data download speed; guarantee the integrity of the downloaded data; improve the utilization of network bandwidth; ensure the robustness of the network.

3. Fragmented dissemination of research content

3.1. Fragmentation design based on Merkel tree

Different blockchain systems may use different block synchronization procedures. Node A can request block synchronization from node B, but it is more difficult. The specific process is as follows (as shown in Figure 1): 1) Node A requests the head of the latest block from node B. This action is achieved by sending a GetBlockHeaders message. Node B will reply to node A a BlockHeaders message containing the block header requested by A. 2) Node A requests the MaxHeaderFetch block to find a common ancestor from node B. The default value of MaxHeaderFetch is 256, but the number of block headers sent by node B to A can be less than this value. 3) If A does not find a common ancestor after the above two steps, node A will continue to send GetBlockHeaders messages, requesting a block header each time. In addition, A repeats in a binary search to find a common ancestor in its local blockchain. 4) After node A finds a common ancestor, A will request block synchronization from the common ancestor. In this process, A requests MaxHeaderFetch block for each request, but the actual number of nodes sent from B to A may be less than this value.

Figure 1. Block interaction process.

Block synchronization based on full nodes generates a large amount of data during the transmission process. If there are more miners in the blockchain network, the generated blocks must be synchronized in the form of broadcast in the entire network, and the data throughput of the entire network is relatively large. At the same time, once the network is hijacked by BGP, it may cause data unreachable, delay data synchronization, and easily cause link bifurcation. Based on the above reasons, we design a fragmentation mechanism in which only the hash value of the transaction and the hash value of the root node are transmitted during the block transfer process, and the hash value of the intermediate nodes is less transmitted, reducing the amount of data. As shown in Figure 2, the N1 and N2 nodes can be combined into one segment, the N0 and N3 nodes can be combined into one segment, and the Root node can be set as a single segment.
3.2. Improve the propagation mechanism, design fragment coding, plan routing

According to the existing Bitcoin network structure, the neighbors of a node (the output can reach 8 and the input can reach 117), so after the sharding is designed, it can be sharded separately according to the number of Merkle tree shards Propagation, that is to say, the route of each slice is different, and it is recombined after reaching the target node. In order to restore the block at the target node, it is necessary to encode the divided slices. Therefore, designing an effective and reasonable dissemination mechanism and matching a reasonable coding method is one of the main contents of the research.

3.3. Perform performance analysis on attack probability and network load

Under the BGP splitting attack or delayed attack model, analyzing the probability of being attacked after the fragments are transmitted will help to further optimize the fragments, and at the same time, it is possible to better design the propagation mechanism. The network load performance analysis is divided into two aspects: one is that the transmission of part of the information can be reduced after the fragmented transmission, and the network load is reduced; the second is that once some fragments are attacked, the attacked fragments need to be retransmitted instead of the entire All blocks are retransmitted, reducing the amount of retransmitted data.

4. Summary

This paper discusses the proposed research content and specific implementation plans in detail, including the reduction of propagation load and block fragmentation, the design and optimization of the parallel block propagation protocol based on fragmentation, and the verification of the parallel propagation mechanism of block fragmentation. Correctness and analyze its performance. We have obtained some preliminary research results for the block data fragmentation and verification of the block data after fragmentation in this article, and the feasibility of its technical route has been preliminarily confirmed from theoretical analysis and simulation experiments; for other research content, Lists the basic ideas to be solved, and has conducted a preliminary analysis of these problems and solutions.

5. References

[1] M. Fadhil, G. Owenson, and M. Adda, “A Bitcoin model for evaluation of clustering to improve propagation delay in Bitcoin network,” in 2016 IEEE Intl Conference on Computational Science and Engineering (CSE) and IEEE Intl Conference on Embedded and Ubiquitous Computing (EUC) and 15th Intl Symposium on Distributed Computing and Applications for Business Engineering (DCABES), 2016, pp. 468–475.
[2] M. Fadhil, G. Owenson, and M. Adda, “Locality based approach to improve propagation delay on the Bitcoin peer-to-peer network,” in *2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM)*, 2017, pp. 556–559.

[3] G. Owenson, M. Adda, and others, “Proximity awareness approach to enhance propagation delay on the Bitcoin peer-to-peer network,” in *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, 2017, pp. 2411–2416.

[4] I. Eyal, A. E. Gencer, E. G. Sirer, and R. Van Renesse, “Bitcoin-ng: A scalable blockchain protocol,” in *13th USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, 2016, pp. 45–59.

[5] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, “Algorand: Scaling byzantine agreements for cryptocurrencies,” in *Proceedings of the 26th Symposium on Operating Systems Principles*, 2017, pp. 51–68.

[6] S. Micali, M. Rabin, and S. Vadhan, “Verifiable random functions,” in *40th Annual Symposium on Foundations of Computer Science* (Cat. No. 99CB37039), 1999, pp. 120–130.

[7] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, “A secure sharding protocol for open blockchains,” in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 17–30.

[8] J. Wang and H. Wang, “Monoxide: Scale out Blockchains with Asynchronous Consensus Zones,” in *16th USENIX Symposium on Networked Systems Design and Implementation (NSDI)*, 2019, pp. 95–112.

[9] M. Apostolaki, G. Marti, J. Müller, and L. Vanbever, “SABRE: Protecting Bitcoin against Routing Attacks,” *arXiv Prepr. arXiv1808.06254*, 2018.

[10] M. Apostolaki, A. Zohar, and L. Vanbever, “Hijacking bitcoin: Routing attacks on cryptocurrencies,” in *2017 IEEE Symposium on Security and Privacy (SP)*, 2017, pp. 375–392.

[11] C. Gkantsidis, J. Miller, and P. Rodriguez, “Comprehensive view of a live network coding P2P system,” in *Proceedings of the 6th ACM SIGCOMM conference on Internet measurement*, 2006, pp. 177–188.

**Acknowledgments**

The paper is funded by Dongguan social science and technology development (general) project (No. 2020507154645) in 2020. Major Scientific Research Cultivation Project of Universities: Research on the Blockchain Fragmentation Mechanism Based on Merkel Tree (GKY-2019CQYJ-13).