A Cascade Structure for Blockchain

Zhuyun Qi[†§], Yan Zhang[‡], Yi Wang[‡§©], Jinfan Wang[‡], Yu Wu[‡]
[†]School of Electronic and Computer Engineering, Peking University, Shenzhen, China, 518055
[†]SUSTech Institute of Future Networks, Southern University of Science and Technology, Shenzhen, China, 518055
[§]Pengcheng Laboratory, Shenzhen, China, 518055
[©]Corresponding Author: wy@ieee.org

***Abstract*—Blockchain as a novel technology which consists of peer-to-peer network, distributed consensus, cryptography and other fundamental knowledge. Blockchain can help people build trust among untrusted people, which will help people establish new application models in multiple areas. But there are several legacy problems which obstruct the deployment and development of blockchain, the biggest problem is blockchain performance that blockchain cannot process the transactions as much as the centralized server per second. We propose a cascade structure for blockchain, which can accelerate the block generation, enlarge the capacity of the block, reduce the risk of fork and increase the difficulty to launch the 51% attack.**

***Index Terms*—blockchain, decentralized system, cascade structure**

I. Introduction

With the flourish of blockchain technology, so many practical fields make attempts to deploy blockchain into their scene that can provide some indispensable properties. But blockchain system has historical issue of performance, which impedes blockchain deployment into some specific areas like the payment transfer, supply chain management, etc.

We design a cascade structure of blockchain which addresses existing performance problems of blockchain. Adding microblocks in parallel between the two key blocks will make block chain a more practical system, which is more suitable for more situations, taking advantage of the new generation of block chain.

II. Problem Statement and Related Work

As we all know, blockchain is treated as a trusted machine to establish the connection among the strangers and protect each participants benefits in a transparent and trustworthy way. In this section, we will list current unsolved problems of blockchain and related works which improve blockchain's performance.

A. Problem statement

- **Limitation of blocks capacity.** Bitcoin, the prototype of blockchain, has the capacity of 1 Mb per block since it was developed. However, with time, Bitcoin becomes famous all over the world, and 1Mb is far from reaching people's needs.
- **Limitation of the consensus.** There is a theory called "Impossible Trinity", which means decentralization, security and scalable cannot achieve at the same time.
- **High transaction fee.** The capacity and other resources limitation force miners of the network choose high-fee transactions to put into the block, which makes low-fee transactions congested in the network.
- **Multicast transmission.** The transaction overlays to the whole network by the multicast way. Due to the logic distances from nodes, it might cost long time to cover over 50% nodes.

B. Related works

Related researchers and engineers are eager to promote the performance to let blockchain has a wide application scenarios. There are two main ways:

1) Changing blockchain structure

In the academia, Bitcoin-NG is an influential project which first proposed that introducing micro blocks between the key blocks to accelerate the block procession, which can reduce the block production period from 10 minutes to 10 seconds. But, as the "Impossible Trinit" said, the security performance will decrease apparently from $1/2$ to $1/3$, because the fork will happen more frequently than the prototype.

There are some other schemes, like using Merkle Partricia Tree and Directed Acyclic Graph (DAG) and so on.

2) Changing the consensus of blockchain

Consensus is the core part of blockchain which determines the nature of blockchain and is the key of building trust among untrusted people. There are several popular consensus deployed over current blockchain project.

- **PoS**, high-speed block commit but it likely makes the strong stronger and the weak weaker. It also suffered from the non-profit attack.
- **DPoS**, which is like a multi-center system, reduces the number of core members to improve the performance.
- **PBFT**, directly transplanted from distributed system, it can also provide high-speed performance, but with the increase of the number of nodes, the performance will be decreased sharply.

There are too many approaches to promote the performance of blockchain that we don't list. In next section, we will introduce the scheme about the cascade structured blockchain.

III. System Design

In this section, we will illustrate the design as Fig. 1 shown. We also utilize the micro blocks which refers to Blockchain-NG, but the differences are the micro blocks are unordered, and transaction-repeat tolerated . The micro blocks between two key blocks are same height, and the production of micro block is irrelevant. The key blocks don't store the transactions

978-1-5386-4870-4/18/$31.00 ©2018 IEEE

but records the digest of micro blocks. We design the following three components to ensure the system work correctly.

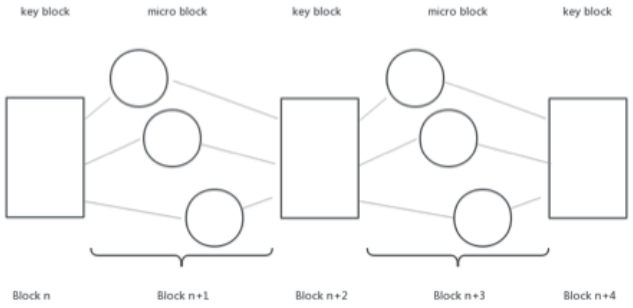

Fig. 1. Cascade structure of blockchain.

A. Consensus system

Due to modifying blockchain structure, the consensus start and end symbols are different. If there is miner $node_a$ who chooses to mine the micro blocks which height are $n+1$, meanwhile many other miners do the same work. When miner $node_a$ receives micro blocks from others with height $n+1$, $node_a$ does not stop mining. When $node_a$ receives key block $n+2$, after verifying key block, $node_a$ will stop current mining and begin the next round consensus. If there is a miner $node_b$ who chooses to mine the key block which height is $n+2$, $node_b$ does not stop mining while receiving micro blocks with height $n+1$, until $node_b$ receives a key block $n+2$ or $node_b$ finishes the consensus by itself, then $node_b$ begins next round consensus. In conclusion, when node receives micro blocks, it does not stop consensus; when node receives key block, they restart consensus immediately, as Fig. 2 shown.

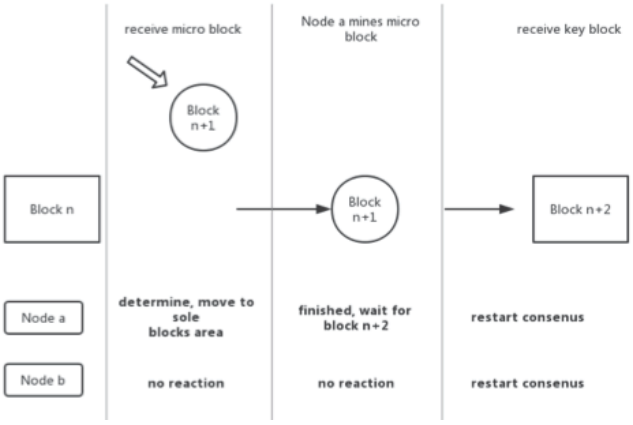

Fig. 2. The different react that node a, node b receive 2 types of block.

B. Block assembly system

Because of 2 different kinds of blocks, the construction of block need to be re-designed. As Fig. 3 shown, the micro block's header is similar to Bitcoin, the only thing should be aware of is there are several micro blocks with the same height. We modified the key block's structure, need to specific parameters ***block_num*** which indicates the micro blocks' number that key block contains, ***previous_hash*** is the latest key block's hash, and non-repeat ***transaction_num*** is the total number of unique transactions.

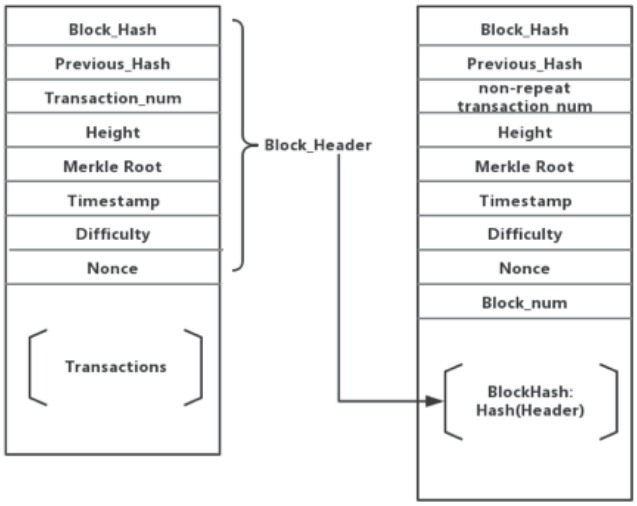

Fig. 3. The structure of block header

C. Block verification system

Every block in blockchain needs to be audited by peers, to verify the validation of transactions and blocks. In our design, the block verification is like following steps:

I. When node receives micro blocks, node will verify the transactions and blocks, then put blocks to the sole block area.
II. When node receives key block, after verifying the key block, node will find all micro blocks recorded by the key block from local sole block area and network.
III. After gathering all the micro blocks, block verification is end.

IV. Discussion

In this section, we will list the advantages of our scheme.

1) Enlarge the transaction throughput: Micro blocks with same height, give each transaction more possibility to be written into blockchain. At the same height, the more micro blocks mean the more transactions.

2) More reliable transaction: Transaction - repeat tolerance model, where a transaction may be stored in a different location microblock. After the micro blocks recorded by the key block, this transaction can be verified multi-times.

3) More computation to launch 51% attack: Because of the same height, micro blocks lead the total difficulty of blockchain upgrade. Although the 51% attack is not eliminated, more computation consumed.

4) Reduce the fork probability: The main blockchain owns the highest difficulty, and half of heights are micro blocks which are fork-tolerated, so only half of the blocks are under the risk of fork.