Estafette

A Parallelized Block Generation Protocol to increase scalability of cryptocurrencies

Ganyuan Cao
Arizona State University
Ganyuan.Cao@asu.edu

Abstract

Cryptocurrencies including Bitcoins and Ethereum are gaining great attention from the whole society. The blockchain technology Bitcoin adopted is also used widely and analyzed in details. However, cryptocurrencies are now usually used in black market and investments nowaday rather than daily use. One of the main reason is that the rate cryptocurrencies process transactions is much lower than established payment service using fiat currency including Visa. Although cryptocurrencies maintain good anonymity of users but it is not enough in current trend of fast payment as well as massive payments through the Internet.

It's necessary to increase the scalability of cryptocurrency through improving current blockchain data structure as well as consensus protocol. We propose a new protocol "Estafette" to enable miners to generate block parallely by modifying the tradition Proof-of-Work algorithm to increase of scalability of cryptocurrency. We compared the performance of "Estafette" with other cryptocurrencies including Bitcoin and Ethereum. And we also compared Estaffete's security with current Bitcoin to ensure it maintains good security.

Introduction

Bitcoin is the first widely used cryptocurrency and the blockchain technology it used spread widely. Many other cryptocurrencies began to follow Bitcoin's success and also proposed a lot of consensus protocols including Proof-of-Stake and protocols based on Byzantine fault tolerance. However, it is notable that transactions throughput and latency of cryptocurrencies are not good enough in current trend of fast and massive payments. For example, VISA handles on average around 2,000 transactions per second while Bitcoin can only process 3-4 transaction.

Current ways of increasing cryptocurrencies' scalability is divided into off-chain solution which is establishing low-tire blockchian through parallelization and on-chain solution which is to modify consensus protocol directly. We proposed a new protocol "Estafette" including on-chain and off-chain solution to increase the scalability of cryptocurrency based on Proof-of-Work algorithm. In Estafette, miners computes partial hash of previous block. Miners can be divided into groups. Each group will compute a specific part of hash of previous block. If a nonce is found to satisfy the target, the block is considered valid. Blocks which can be generated parallely are considered as child blocks while there are still parent blocks computed with whole hash of previous block to as the container to lead those child blocks. In addition to parallelized block generation, we also proposed sharding transactions consensus by forming committee lead by the miner who worked out child blocks with Byzantine fault tolerance scheme.

Mining with Proof-of-Work

In the original Proof-of-Work algorithm, mining is completed by solving a cryptographic puzzle which is finding the value of nonce with previous hash(hash value of previous block) with the SHA-256 function. Each miner uses the nonce to yield a target hash. The mining difficulty is a 32-bit integer that compresses the actual hex target. It consists of two parts : exponent and coeffcient C.

$$Target = C * 2^{(8*(exponent-3))} \tag{1}$$

For example, the block number is 421133. The value of difficulty is 402990845 and in hex is 0x180526FD. The coeffcient is 0x0526FD and the expoent is 0x18. The target is :

$$Target = 337661 * 2^{168} = 0x000\cdots0000526FD0\cdots0 \tag{2}$$

Miners must work out the hash value lower than the target above such that the block is considered valid.

Block Structure

There are 2 types of block in Estafette : parent block and child blocks. Parent block and child blocks can be generated parallely. Parent block contains previous hash from previous block, nonce, child hash computed from child blocks and number of transactions it can hold.

Parent block does not directly contain transactions. Number of transactions in the block can be predefined. The number of transactions is the sum of all transactions in child blocks.

Child block contains partial previous hash, nonce and transactions. Number of transactions in child block may not be the same. But the sum of number of transactions in all child blocks must be the same as predefined in parent block.

Multiple parent blocks can also be generated at the same time if and only if the nonces miners find for parent block satisfy the specified target.

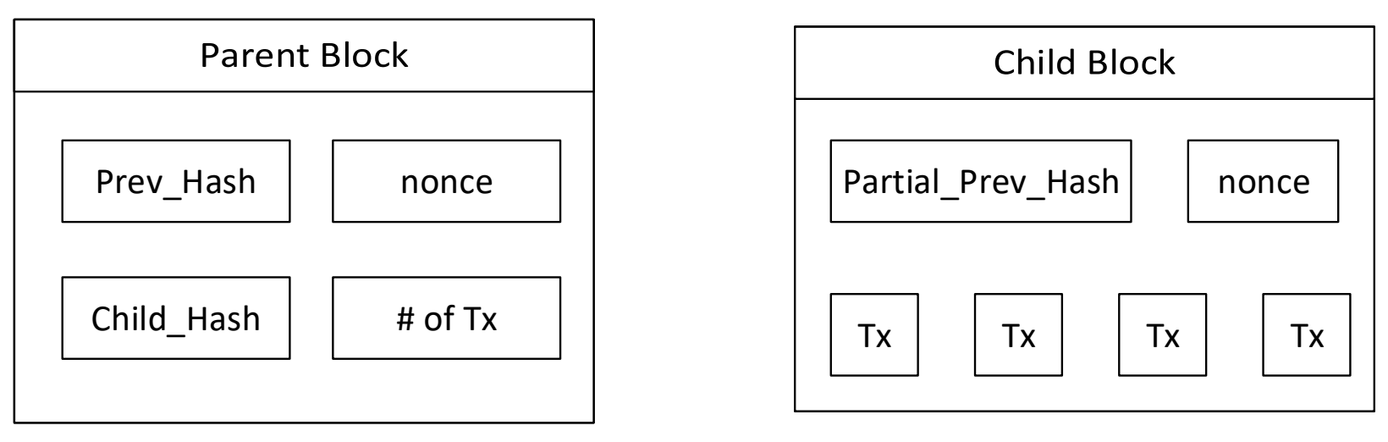

Figure 1: block structure

Chaining Method

Parent block acts a container for child blocks. Chaining between parent blocks is the same as Proof-of-Work. Chaining between child blocks and their parent block is done by calculating the hash of child blocks and including it in parent block. Estafette established cryptographic pointer between parent block and parent block as well as between parent block and child blocks similar with Proof-of-Work algorithm.

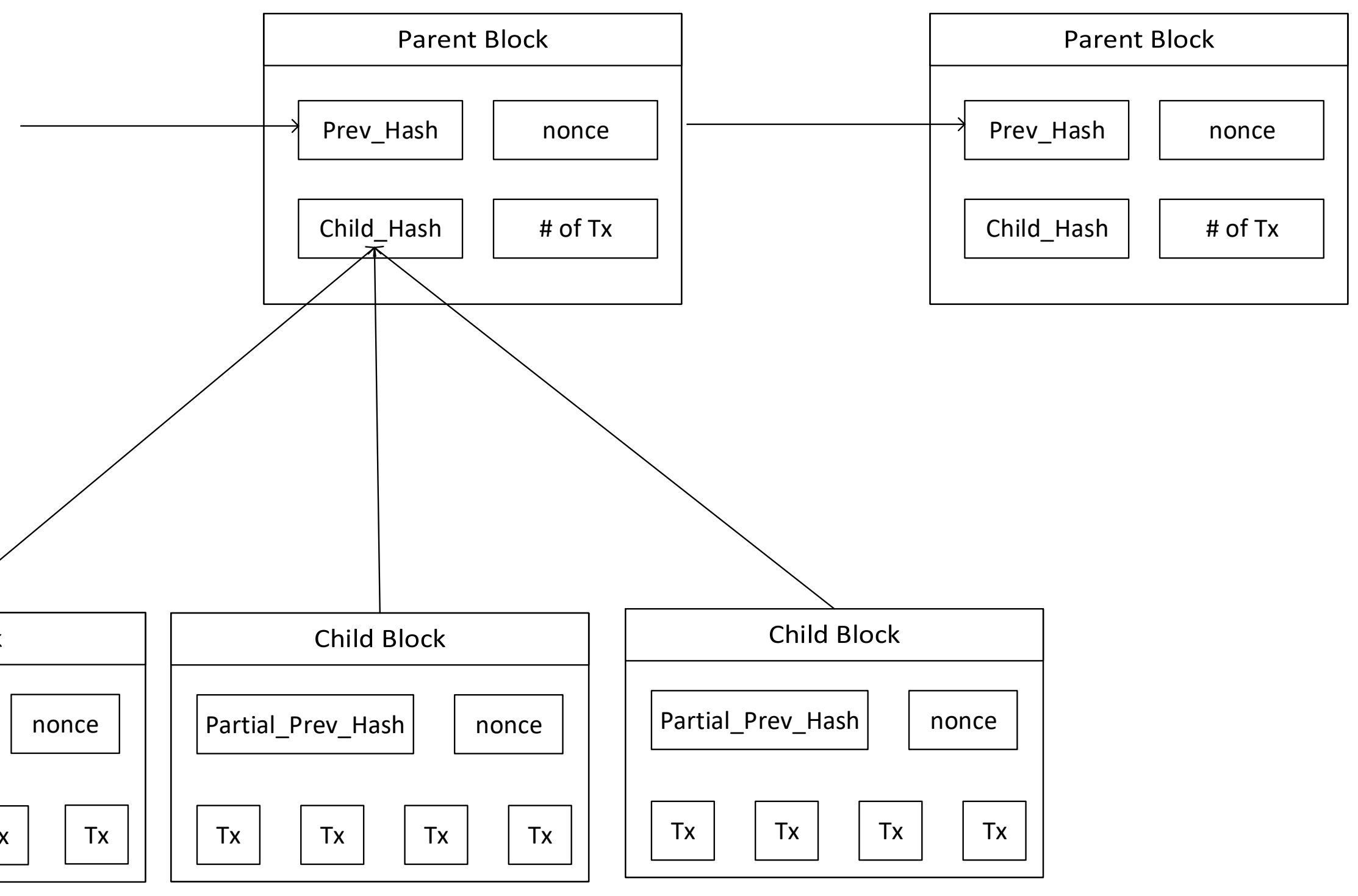

Figure 2: chain structure

Block Generating

Parent blocks are generated following traditional PoW, which is computing a nonce to yield a specific target.

Child blocks are generated by computing a nonce for random partial string of previous hash to satisfy a specific target.

1. Multiple child blocks can be generated parallely since they are assigned different partial strings from previous hash.
2. Child blocks and their parent block can be generated at the same time. Child block do not need to wait before their parent block is generated. They could work on their own computing for their own nonce.

Child blocks are set difficulty from the parent block , which makes it possible to have multiple child blocks are generated at the same time with parent block. For example, consider the target for the parent block, the target is :

$$Target = C * 2^{(8*(exponent-3))} \tag{3}$$

Assume for a parent block, there exist n child blocks in total, the mining difficulty for each of them is $\frac{Target}{n}$.

Consensus Model

1. Based on predefined number of transactions, an Epoch is defined as :
   a. Generate a parent block and several child blocks
   b. Each child block committee agree on a group of transactions
   c. Transactions are confirmed in every child blocks
   After an Epoch ends, another Epoch starts immediately.

2. Leader selection and Committee formation :
   Transactions are broadcast through gossip network before child blocks are generated. After a child block is generated, the node who worked out the block will be the leader of that child block committee. Other child blocks will choose $\frac{1}{n-1}$ part of members for a child block where n is the total number of child blocks. For example, after 4 child blocks are generated, each leader of the other three child block committees will choose $\frac{1}{3}$ part of members for the remaining child block's committee.

Conclusions

Estafette is a parallelized block generation protocol for the cryptocurrency. Using Estafette can reduce the time of mining blocks during the consensus of transitions and increase the scalability of cryptocurrency by using the parallel blockchain structure. Estafette also provides good security in the decentralized environment by adopting Byzantine fault tolerance. In conclusion, Estafette is a new protocol for cryptocurrency to increase its scalability and consensus efficiency as well as perverse good security.

Forthcoming Research

Further research needs to be complete in the following aspects :

1. Choose the proper size of committee members for each of the child block.
2. Choose the proper maximum number of child blocks included in parent block.
3. Set the proper hash target for different child blocks.

Reference

Xue, Tengfei, Yuyu Yuan, Zahir Ahmed, Krishna Moniz, Ganyuan Cao, and Cong Wang. "Proof of Contribution: A Modification of Proof of Work to Increase Mining Efficiency." In 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), pp. 636-644. IEEE, 2018.