ISBN 978-981-11-7861-0
Proceedings of 2018 the 8th International Workshop on Computer Science and Engineering (WCSE 2018)
Bangkok, 28-30 June, 2018, pp. 411-416
doi: 10.18178/wcse.2018.06.072

Research of Merged Mining Technology in Bitcoin Blockchain Scaling

Xue Zhipeng, Duan Xuliang and Wen Zheng

School of information engineering, Sichuan Agricultural University, ya'an 625014, China

Abstract. Bitcoin is a digital currency raised by Satosghi Nakamoto, which is Completely decentralized, Highly anonymous, cross-border. Nowadays it has became one of the most widely used currency. Recently, as the used capacity has approached the capacity limitation of each block, the time needed to confirm a transaction increase dramatically. As a result, bitcoin cannot satisfy the need of a large number of bitcoin transactions. This paper aims to apply merged mining technology to bitcoin blockchain scaling, which builds another blockchain called auxiliary blockchain based on bitcoin blockchain and stores some of small rapid transactions in auxiliary blockchain. This paper also proves the merged mining technology can concentrate computing power and design a special miner reward program.

Keywords: blockchain, bitcoin, merged mining technology, auxiliary blockchain.

1. Introduction

Bitcoin is a new type of decentralized digital currency designed by Nakamoto in November 2008 as a highly anonymous decentralized currency[1].However, as bitcoin is used widely, the requirement of its performance increases continually, and its drawback of insufficient capability is exposed gradually.

Since 2012, the size of each block has continued to increase. In 2015, the growth speed of block size has peaked, doubling the median volume of single block size. By 2016, the median volume of a block size has reached 994KB, about 16 percent of transaction have waited for more than one hour and even one percent of transactions have waited for more than one day[2], which affect the user experience seriously.

To solve this problem, the bitcoin forum has proposed several BIP(Bitcoin improvement protocol).For example, BIP101 suggests to increase the block capacity at a predictable speed instead of using fixed maximum block capacity, solving the insufficient capacity problem once and for all[3]. Bip102 suggests to increase the block capacity from 1MB to 2MB directly, alleviating the current lack of capability of the block[4].BIP141 designs the segregated witness program, which separates signature data stored in the same data structure with transaction data and save them separately.This program can disguised scale the block capacity[5].However, the paper[6]points out that the block size can not be increased indefinitely, due to the limitation of network bandwidth, the large block will increase the time required to spread to the whole network, the increasing spreading time will affect the consensus mechanism and lead to the problem of high individual block rate.

In May 2017, 58 organizations signed the New York Agreement and started Segwit2x project, which aims to setup the segregated witness program and increase the block capacity to 2MB by hard fork[7].In November 2017, one of the principal manager of Segwit2x project, Mike Belshe announced the failure of the hard fork because of insufficient consensus by e-mail[8].

In summary, although there are several programs proposed by bitcoin forum, because of the lack of feasibility and insufficient consensus, the problem of block capacity limitation is still unsolved.

+ Corresponding author. Tel.: + 86 150-0830-5394
E-mail address: duanxuliang@sicau.edu.cn

The main contributions of this paper are applying the merged mining technology into bitcoin blockchain scaling problem, giving a programme of scaling according to the format and required parameters of merged mining technology, proving the merged mining technology can concentrate more computing power on calculating for blockchain and discussing the miner reward of merged mining technology.

2. Background Knowledge Of Blockchain

2.1. Transaction

There are three kinds of transactions of bitcoin, including Generation Transaction, Script Hash Transaction, Pubkey Hash Transaction. The Generation Transaction is the first transaction of a blcok, its output is the new bitcoin and its input is a special parameter ”coinbase” , which can be written in any value.The Script Hash is a rarely used kind of transaction, its address is created by three pairs of public and private keys. People can use the bitcoin from such address by just one private key. Pubkey Hash is the most widely used kind of transaction, it includes N inputs and M outputs.

2.2. Block

Each block consists of a header and a body. The header of a block includes the current vision number, the root of Merkle tree, which is a special binary tree and its nodes are the hash of the transactions stored in current block,the hash of previous block, the Unix timestamp of the block creating time,the hash difficulty used for POW(Proof-Of-Work) and a random value.The body of block stores the detailed information of each transaction. The average time of block interval is ten minutes, and the capacity of a block is 1MB.

2.3. The Chain Structure Of Blocks

The chain structure of blocks is a structure that consists of the blocks which contain all the information of its previous blocks based on the Secure Hash Algorithm.After achieving the target hash difficulty, the node will broadcasts to the whole network, and other nodes will verify the result, if the result truly satisfy the hash difficulty, they will download the new block and calculate the new target hash. As each block contain the hash of previous block, node can make sure the history transaction information haven’t been changed under the chain structure of blocks.

2.4. Miner Reward

The operation of blockchain is maintained by all the nodes.Bitcoin set hash difficulty for POW and the attack to the bitcoin won’t be successful unless the attacker has more than 51 percents of computing power.So, in order to inspire the miner to provide sufficient computing power for bitcoin blockchain, it will reward the miner who find a new block with some bitcoins.

3. The Merged Mining Technology In Blockchain Scaling

Merged mining technology means building another blockchain——auxiliary blockchain, based on the original blockchain——parent blockchain and auxiliary blockchain trusts parent blockchain’s work as its own. When a node finds a hash which satisfies auxiliary blockchain’s hash difficulty but not satisfies parent blockchain’s hash difficulty, the node will broadcast to the auxiliary blockchain network. When a node finds a hash which both satisfies auxiliary blockchain’s and parent blockchain’s hash difficulty, the node will broadcast to the parent blockchain network. As a result, the node will provide both auxiliary blockchain and parent blockchain with computing power and it can ensure their safety at the same time.In the merged mining technology, the parent blockchain doesn’t need to change anything but auxiliary blockchain need specific design to execute AuxPOW（Auxiliary Proof-of-Work）protocol.

In 2014, The hard fork that enables AuxPoW kicked in at block 371337 of dogecoin. The dogecoin changed into a auxiliary blockchain of litecoin, which prevent the crisis of too little computing power in dogecoin blockchain[9].

3.1. The Requirement and Format of Merged Mining Technology

The mainly difference between AuxPOW and POW is that AuxPOW doesn’t have clear hash difficulty but AuxPOW needs to meet two conditions:

(1)The hash of auxiliary blockchain must be stored in parent blockchain's "coinbase" parameter.

(2)The hash difficulty of parent blockchain must be higher than that of auxiliary blockchain.

For one hand the several parameters required to be written in parent blockchain's "coinbase" parameter are as listed:

Table 1: Parameter written in coinbase

Description	Size	Data type	Comment
magic	4	char[4]	0xfa, 0xbe, 'm'
aux_block_hash	32	char[32]	Hash of auxiliary block header
merkle_size	4	int32_t	Number of transaction auxiliary block Merkle tree
merkle_nonce	4	int32_t	Nonce used to calculate indexes into auxiliary block merkle tree

For another hand, the auxiliary block need add additional five parameters based on the current structure of transaction.

Table 2: Additional five parameters in auxiliary block transaction

Description	Size	Data type	Comment
coinbase_txn	?	txn	Coinbase transaction that is in the parent block
block_hash	32	char[32]	Hash of the parent block header
coinbase_ branch	?	Merkle branch	The merkle branch linking the coinbase to the parent block's Merkle root
blockchain_ branch	?	Merkle branch	The merkle branch linking this auxiliary blockchain to the others
parent_block	80	Block header	parent block header

The node can verify the AuxPOW through following three processes:

(1)Verify whether the header of parent block satisfies auxiliary block hash difficulty.

(2)Verify whether Generation Transaction is contained by parent block.

(3)Verify whether the hash of auxiliary block is written in coinbase parameter[10].

3.2. The Principle of Scaling

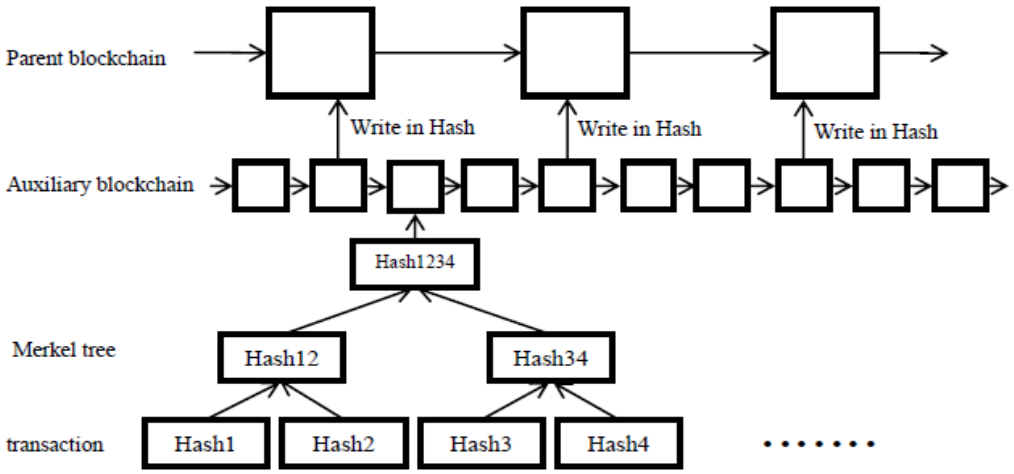

Fig. 1: The principle of scaling.

Firstly, according to the format of merged mining technology, build another blockchain as a auxiliary blockchain, whose time of block interval can be less than ten minutes and capability can be more than 1MB.Secondly, divide all the transactions into two types, one is large transaction which need to be more safe and another is small transaction which need to be verify rapidly Then put the first type of transactions into the parent block——bitcoin blockchain, and put the second type of transaction into the auxiliary block.When the parent blockchain creates a new block, write the hash of auxiliary blockchain into "coinbase" to ensure the safety of small transactions. As there is no need to change the parent blockchain, so apply merged mining technology to bitcoin blockchain scaling will not lead to any fork.

3.3. Increasing Computing Power

When there is one blockchain, the blockchain will execute in the serial process of verifying hash difficulty, downloading the block, calculating the hash. However, when there is another auxiliary blockchain, it can divide a big block into several small blocks, downloading the block and calculating the hash at the same time, which can gather more computing power.

When there is only one blockchain, the average time of blocks interval is t_1, the time to download the block is x_1, the computing power of the whole network is w, so the calculation of each block is $w(t_1 - x_1)$

When there is a parent blockchain and a auxiliary blockchain, the average time of parent blocks interval is t_1, the average time of auxiliary blocks interval is t_2, the time to download parent block is x_2, the time to download auxiliary block is x_3, the calculation of parent block is $w(t_1 - x_2)$, the calculation of auxiliary block is $w(t_1 - x_2)(t_2 - x_3)/t_2$

We assume the condition of network will not change in a short time, and the speed of downloading is v

When the storage transaction data in the first situation is equal to that in the second situation, which means $x_2 + (10 - x_2)x_3/t_2 = x_1$

At this time, it is clear that $w(t_1 - x_2) > w(t_1 - x_1)$

In conclusion, merged mining technology can increase the computing power of parent blockchain and decrease the lack of attack.

3.4. Miner Reward

In order to encourage miners to provide bitcoin blockchain with sufficient computing power to maintain its operation, it will send some of new bitcoins to the miner's address who finds a new block as reward. The source of revenue of miners are the reward from the blockchain and the fee of bitcoin transaction. The bitcoin blockchain generates 50 bitcoins a block at the beginning, then halves the bitcoin generated every four yeas untill 2140, and there will be no reward for finding a new block after2140. At that time, the revenue will only come from transaction fee[11].

To prevent to create new bitcoin or other competition coin, the auxiliary block will not reward the miner when he finds a new block but he can get some percents of transaction fee. It is clear that if the revenue from auxiliary blockchain more than parent blockchain, the miners will stop calculating for the parent blockchain but only calculate for auxiliary blockchain. In order to prevent the attack from auxiliary, and gather more than 51 percents of computing power for parent blockchain, the revenue from parent blockchain should be more than 51 percents of all the reward.

4. The Comparison of Other Programme

The RSK(rootsock) uses the technology with sidechain,which builds another blockchain and is two-way wagged with the main blockchain. There is a kind of bitcoin token called smartBTC, and its exchange rate is smartBTC:BTC=1:1. when users use bitcoin to trade with each other, they need to seed their bitcoin to a semi trusted third party and they will send the smartBTC to users on the sidechain. after the transaction, users send smartBTC to the semi trusted third party and they will send BTC to users on the main blockchain [12,13].

Extension blocks devise a second layer on top of canonical bitcoin blocks, and it will control the transaction enter or quit the extension blocks according to a parameter[14].

	Extension blocks	RSK	Merged Mining
Fork	√	×	×
Semi trusted third party	×	×	×
Smart contrast	×	√	√
Competitive coin	×	√	×

5. Prospect

As a parent blockchain can have indefinitely auxiliary blockchains, the merged mining technology can give chance to bitcoin to build smart contract system which is impossible because of insufficient capacity. smart contract is proposed by Nick Szabo in 1997[15], which is a highly evolved e-commerce contract between online strangers. Under the smart contract system, bitcoin can be used in more occasions such as medical area, financial area, etc.

6. Conclusion

The merged mining technology can solve the problem of bitcoin blockchain scaling effectively by building another auxiliary blockchain with appropriate parameters and special miner reward programme.The large transactions stored in parent blockchain can be more safe as the merged mining technology can concentrate more computing power and the small transactions stored in auxiliary blockchain can be verified rapidly.What's more, the merged mining technology can build a smart contrast system which can lead a wider use of bitcoin.

7. Acknowledgement

The authors thank some helpful work from Wu Yi, Mou Yunjing, Liu Xiaobao. They also thank the suggestion and instruction from Prof. Zhang Dejun

8. References

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf, retrived December. 2017.

[2] Yu Hui, Zhang Zongyang, Liu Jianwei. Research On Scaling Technology Of Bitcoin Blockchain. In *Journal Of Computer Research And Development*(2017).

[3] Andresen G. BIP 0101:Increase maximum blocksize., https://github.com/bitcoin/bips/blob/master/bip-0101.mediawiki, retrived December. 2017.

[4] Garzik J. BIP 0102:Block size increase to 2MB. https://github.com/bitcoin/bips/blob/master/bip-0102.mediawiki, retrived December. 2017.

[5] Lombrozo E, Lau J, Wuille P. BIP 0141:Segregated Witness (Consensus layer). https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki, retrived December. 2017.

[6] Croman K, Decker C, Eyal I, et al. On Scaling Decentralized Blockchains. In *Financial Cryptography and Data Security*(2016).

[7] Haywood M. Segwit2x, 'The New York Agreement'. https://bravenewcoin.com/news/segwit2x-the-new-york-agreement/, retrived December. 2017.

[8] Belshe M, [Bitcoin-segwit2x]Segwit2x Final Steps. https://lists.linuxfoundation.org/pipermail/bitcoin-segwit2x/2017-November/000685.html, retrived December. 2017.

[9] Higgins S, Dogecoin Community Celebrates as Merge Mining with Litecoin Begins.https://www.coindesk.com/dogecoin-celebrates-litecoin-merge-mining/, retrived December. 2017.

[10] Nakamoto S. Merged mining specification. https://en.bitcoin.it/wiki/Merged_mining_specification, retrived December. 2017.

[11] Buterin V. Satoshi's Genius: Unexpected Ways in which Bitcoin Dodged Some Cryptographic Bullets. https://bitcoinmagazine.com/articles/satoshis-genius-unexpected-ways-in-which-bitcoin-dodged-some-cryptographic-bullet-1382996984/, retrived December. 2017.

[12] Back A, Corallo M, Dashjr L. Enabling blockchain innovations with pegged sidechains. https://blockstream.com/sidechains.pdf, retrived December. 2017.

[13] Sergio D.RSK White Paper Overview. https://uploads.strikinglycdn.com/files/ec5278f8-218c-407a-af3c-ab71a910246d/RSK%20White%20Paper%20-%20Overview.pdf, retrived December. 2017.

[14] Christopher J, Joseph P, Fedor I, et al.Extension Blocks. https://github.com/tothemoon-org/extension-blocks/blob/master/spec.md, retrived December. 2017.

[15] Szabo N. Formalizing and Securing Relationships on Public Networks. http://ojphi.org/ojs/index.php/fm/article/view/548, retrived December. 2017.