Dynamically Adjusting the Mining Capacity in Cryptocurrency with Binary Blockchain

Yoohwan Kim[1], Ju-Yeon Jo [2]

[1] *University of Nevada Las Vegas*
4505 S. Maryland Parkway
Las Vegas, NV 89052, USA
E-mail: Yoohwan.Kim@unlv.edu

[2] *University of Nevada Las Vegas*
4505 S. Maryland Parkway
Las Vegas, NV 89052, USA
E-mail: Juyeon.Jo@unlv.edu

Abstract

Many cryptocurrencies rely on Blockchain for its operation. Blockchain serves as a public ledger where all the completed transactions can be looked up. To place transactions in the Blockchain, a mining operation must be performed. However, due to a limited mining capacity, the transaction confirmation time is increasing. To mitigate this problem many ideas have been proposed, but they all come with own challenges. We propose a novel parallel mining method that can adjust the mining capacity dynamically depending on the congestion level. It does not require an increase in the block size or a reduction of the block confirmation time. The proposed scheme can increase the number of parallel blockchains when the mining congestion is experienced, which is especially effective under DDoS attack situation. We describe how and when the Blockchain is split or merged, how to solve the imbalanced mining problem, and how to adjust the difficulty levels and rewards. We then show the simulation results comparing the performance of binary blockchain and the traditional single blockchain.

Keywords: Blockchain, Cryptocurrency, Bitcoin, Scalability, Parallel Mining.

1. Introduction

Since the introduction of the first cryptocurrency Bitcoin, many other cryptocurrencies have been created. To avoid a double spending problem, the majority of cryptocurrencies employ a distributed public ledger called Blockchain [5]. In this scheme, multiple transactions are grouped into a block, and it is then appended to the previous blocks continually, creating a chain of blocks, hence it is called Blockchain [2]. The structure of a typical block is shown in Fig. 1. To prevent an arbitrary addition of a block into the blockchain, there is an essential process called *mining*. Before adding a block to the existing blockchain, a signature value must be discovered that produces a particular style of hash value. Specifically, it is a hash operation that takes the input of the summary hash of all transactions within the block and the previous block's hash value. In addition, a nonce value is added and a new hash value is calculated. This process continues with a new nonce value until a special nonce value is found that produces a hash value beginning with a predetermined number of 0's.

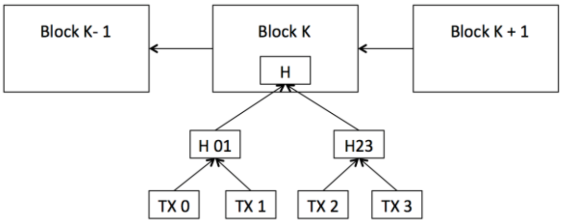


Fig. 1 Blockchain structure

Any individual or organization with adequate computing resources, called miners, may attempt to find the signature value. There are thousands of miners in the

Bitcoin mining network and they compete to find a signature value. When a miner finds a signature value successfully, he or she can attach the block to the Blockchain and is rewarded with new cryptocurrency [9]. The block generation and mining process is described in Fig. 2.

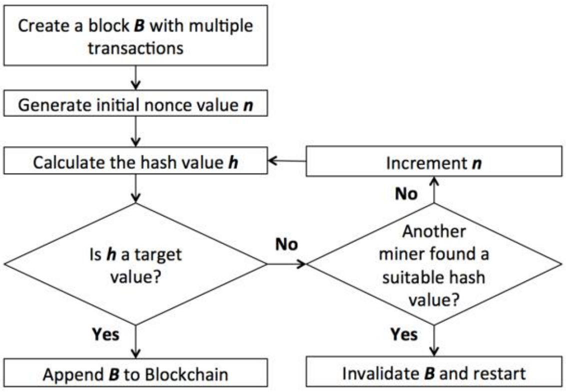

Create a block ***B*** with multiple transactions
Generate initial nonce value ***n***
Calculate the hash value ***h***
Increment ***n***
No
Is ***h*** a target value?
No
Another miner found a suitable hash value?
Yes
Yes
Append ***B*** to Blockchain
Invalidate ***B*** and restart

Fig. 2 Mining process

Unfortunately, this mining process was not designed with scalability in mind. In case of Bitcoin, the blocks are generated approximately every 10 minutes and the maximum block size is 1MB. If the average transaction size is 500 bytes, about 2,000 transactions can be placed in each block, giving the processing speed of about 3.3 transaction/sec [27][11]. Another popular Cryptocurrency, Ethereum, uses a slightly different method, and it can achieve the maximum of 15 transactions per second [1]. Compared with commercial credit card processing speed that easily surpasses 10,000's transactions per second, cryptocurrency mining speed is very slow, creating scalability problem. [10][19][21][28]. This limited mining capacity created a big backlog of unconfirmed transactions and increased the transaction confirmation times recently [4][16]. In May 2016 it was generally below one hour, but in May 2017 it often exceeded 10 hours. Furthermore, the transaction load can be increased abnormally in certain situations such as DDoS attacks, which can create an enormous backlog for legitimate transactions. Mining congestion also caused an increase in the mining fees because miners are more inclined to include those transactions with higher fees in their blocks. Mining congestion is becoming more problematic, as it is limiting the growth of Bitcoin and other similar cryptocurrencies that employ blockchain. While several methods have been proposed, they are still being debated.

We propose a simple method to dynamically adjust the mining capacity based on the mining congestion level. In this scheme called Binary blockchain, we increase the number of chains when the load goes up, and reduce it when the load comes down. Due to the nature of binary division, its mining capacity can be easily increased by an order of thousand. In this paper, we describe the process of Binary blockchain management and related issues. We then compare the performance of Binary blockchain with those of the traditional Blockchain through simulation study.

2. Efforts to Increase Mining Capacity

The topic of mining capacity scalability is actively discussed in the blockchain community [26]. We will review some of the proposed methods in this section.

2.1. Increasing the Block Size

The most obvious solution is to increase the block size and there are multiple proposals on that [6][23]. One of the proposals, Bitcoin Cach (BCH), increases the block size to 8MB. While this can temporarily increase the mining capacity, the same problem will be faced again if the Bitcoin transactions grow continuously. But it is impractical to increase the block size continuously due to the network bandwidth limitation and propagation delay. [12] pointed out that each kilobyte in block size adds 80 *ms* delay until the majority knows about the block while another research [24] suggested 8ms of delay.

2.2. Decreasing the Block Mining Period

Another solution is to decrease the block confirmation time. The downside of this approach is the increased probability of fork and orphaned blocks. Currently, bitcoin block confirmation time is 10 minutes and forks are created a few times per week on the average. Litecoin has proven the viability of a shorter confirmation time of 2.5 minutes, where its probability of having a fork is not very different from Bitcoin's. Ethreum's mining period is much shorter, 14 seconds on the average, which increases the chance of orphaned blocks significantly (called uncle blocks) to near 2% [8]. Although the mining period is much shorter in

Ethereum, the block size is also much smaller (less than 20kB) with about 200 transactions per block. This gives a 3 to 4 times higher processing rate (~15 transactions per second) than Bitcoin (3 to 7 transactions per second). The block mining period cannot be shortened infinitely either due to the network capacity and propagation delay, as it may cause too much instability to the mining network.

2.3. Alternative Data Structure for Blocks

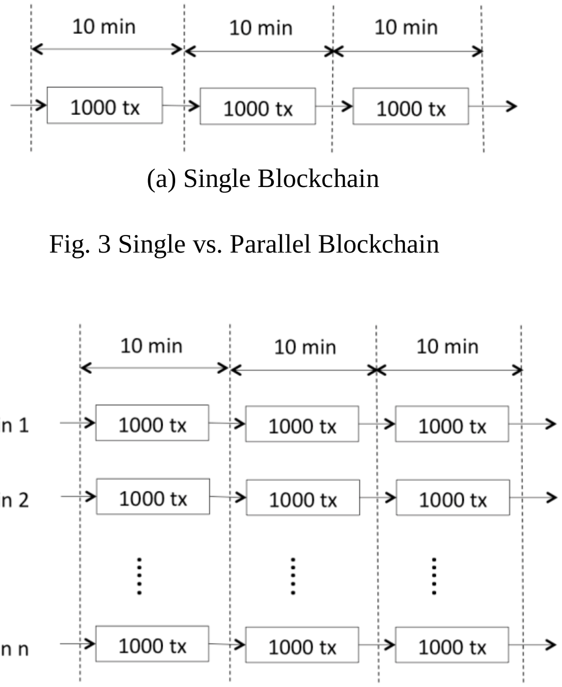
Instead of putting the complete transaction information, only the most essential piece of information may be placed in the block. This reduces the amount of storage, and increases the number of transactions in the block. SegWit (segregated witness) moves some non-critical data, called witness data, out of transactions and off the Blockchain. While it can immediately increase the capacity, it will eventually face the same problem with the limited block size.

2.4. Off-Chain Transactions

Some methods are used to offload transactions from the blockchain, such as off-chain transactions [22][26], side chain, merged mining, etc. SegWit also allows a second layer such as the “lightning network” where sequences of transactions can be started on the blockchain, then continued outside of it without using network bandwidth. However, these methods do not address the capacity of the mining network itself directly. Other solutions have been proposed, such as separating the Bitcoin functions on different chains and blocks [14][15][18][20]. While they offer a scalable solution, they may depend on other factors such as a larger block size (e.g., 32 MB) to realize sufficient scalability.

2.5. Parallel Mining with Transaction Partitioning

Another approach is to allow multiple branches to confirm the blocks simultaneously on a disjoint set of transactions. Binary sharding has been discussed in the Ethereum community, but the details are still being developed. The idea of Tree Chain was proposed earlier [25], but was only conceptualized and has not progressed enough for further debate. It suggested a tree-structured blockchain where each branch can mine blocks, but the structure is static and cannot respond to the dynamically changing transaction load. The use of a DAG (Directed Acyclic Graph) structure instead of a tree structure has also been proposed. MultiChain [7][17] has an aspect of parallel mining, but it is across different blockchains, not in the same blockchain. These parallel mining techniques can increase the mining capacity without increasing the block size or reducing the block mining time, as shown in Fig. 3, but they also bring up some challenges as outlined in the next section.



(a) Single Blockchain

Fig. 3 Single vs. Parallel Blockchain

(b) Parallel Blockchain

3. Issues with Parallel Mining

In this section, we will discuss the problems and possible solutions in parallel mining.

3.1. Preventing Double Spending

In a traditional single-chained blockchain, parallel branches or fork may occur inadvertently while the blockchain information propagates throughout the mining network in p2p fashion. Since it can create a double spending problem, only one branch must be chosen. The mining network chooses the longest branch between them, and the orphaned blocks get invalidated.

In parallel mining, multiple branches are created on purpose, and double spending may be possible if the same transaction gets included in multiple branches. To avoid this, the transactions must be divided into disjoint groups. Binary sharding based on the transaction ID or hash value can be employed for this purpose.

3.2. Authority to Create and Delete Chains

To cope with the varying transaction load, the number of parallel chains must be increased or decreased. In public Blockchain, this decision cannot be made by a single central authority. So the decision to create or delete the chains must be embedded in the Blockchain itself.

3.3. Difficulty Level Adjustment

In Bitcoin, the difficulty level of the mining is adjusted periodically (about every two weeks) to make the average block confirmation time 10 minutes. Under parallel mining, the mining resources are divided into multiple groups, and consequently, the conformation time will increase with smaller resources. Therefore, the difficulty level must be reduced accordingly to maintain the 10-minute confirmation time.

3.4. Reward Re-allocation

With parallel mining, there are multiple branches at the same time. If the reward amount per block stays same, the total reward will increase, which will violate the design principle of the current Bitcoin system. To prevent it, the size of the reward must be divided by the number of parallel branches so that the total reward is same as in the single blockchain.

3.5. Risk of Unbalanced Mining

If the miners are not evenly distributed among the parallel branches, two problems may occur.

- Over-mining on one branch: Intentionally or unintentionally, all miners may concentrate on one branch. Then the confirmation time for a block will be much shorter than 10 minutes. This increases the possibility of fork and more orphaned blocks, and cause starvation on the other branch where little mining operation is performed.
- Easier 51% attack: A mega-miner can concentrate on one branch and launch a 51% attack more easily.

To avoid these risks, there must be a way to spread the miners evenly over the multiple parallel branches.

4. Proposed Method: Binary Blockchain

We propose a method that can dynamically adjust the mining capacity based on the mining congestion level. The process of creating and merging the subchains is described in Algorithm 1.

Algorithm 1: Block Creation with Division and Merge

```
Input:    T (the set of transactions), C (existing Binary blockchain)
Output:   B (new block)
1   // Choose a subchain
2   Choose any subchain from C (or main chain if there is only one chain)
3   // Check for division
4   If division conditions are met
5       Decide which subchain to follow between new subchains
6   Else
7       Follow the current subchain
8   End
9   // Check for synch block
10  If the block B to be created is a synch block
11      If the hash values from all sibling pre-synch blocks are available
12          Inherit them all
13      Else
14          Go to 2 (Choose another subchain from C and re-start)
15      End
16  Else
17      Inherit hash value only from the preceding block
18  End
19  //Check for merge
20  If merge conditions are met
21      Inherit hash from both subchains
22  Else
23      Inherit hash value only from the preceding block
24  End
25  // Block numbering
26  Assign an appropriate block number to the new block B
27  // Transaction sharding
28  Choose eligible transactions from T for the new block B
29  // Perform mining
30  Confirm block B, and add it to the chosen subchain if confirmed
```

We will use the terminology defined in Table 1.

Terms	Definition
Traditional chain	The single original blockchain
Branch	Temporarily competing blockchains in the traditional blockchain
Fork	Process of creating branches (unintentionally)
Main chain	A linear portion of Binary blockchain
Parent chain	A portion of Binary blockchain before division
Child(ren) chain	A portion of Binary blockchain after division
Subchain	Same as child(ren) chain
Sibling chains	A pair of subchains
Division	Creating a pair of chains
Merge	Combining a pair of subchains into one chain

Table 1. Definitions

4.1. The Concept

A binary Blockchain increases the mining capacity by twice when the mining pool is split, or decreased when the pool is merged. A new blockchain is not created additively, but by a binary division of the existing chain. When there is a split, the level of chain increases. The level k = 0 for the single Blockchain. At first split, k=1, and there are 2 chains. At second split, k=2, and there are 4 chins, and so on.

Each subchain can be split further or merged independently based on its own transaction load. When it is split, both new blocks inherit the hash value from the parent block, thus maintaining the continuity of the blockchain. When two chains are merged, the merged chains inherit hash values from both parent blocks.

The key concepts of binary Blockchain are:

- Binary sharding of transactions: The transactions can be divided into disjoint groups for each subchain based on their hash values with simple modulo operation by the level of subchain. We apply binary sharding as following.
  - The number of groups = 2^k
  - Group id for trans n = trans id % 2^k
- Difficulty level adjustment: The difficulty level gets halved for each division. This increases the overall mining capacity by a factor of two.
  - Difficulty level at level k = original difficulty * 2^{-k}
- Reward calculation: The reward gets halved for each division. This ensures that the amount of total rewards stays same as in the traditional blockchain regardless of the number of subchains.
  - Reward for mining a block at level k = original reward * 2^{-k}
- Balanced mining: Balanced mining can be maintained systematically with the synch blocks. The distance between synch blocks increase by power of 2 after each division.

Although it may look similar, Binary blockchain is different from TreeChain in that the whole blockchain or each subchain can dynamically and independently increase or decrease. It is also different from side chain or data sharding.

4.2. Block Numbering

Since the blockchain is not linear any more, we need to number the blocks differently. We use a hierarchical numbering format of "n1.n2.n3.….", where a division is marked by a period symbol (".") and each number indicates the location within the subchain. The block number increases only within the last subchain level. In Binary blockchain, two subchains (top and bottom) are created upon division, and we need to differentiate them. For that, we divide the numbers in two groups (odd and even) and assign them to each subchain. In the top subchain, the block numbers grow in even numbers (0, 2, 4, …), and in the bottom subchain, they grow in odd numbers (1, 3, 5, …). When the subchains are merged, the last level subchain block number is removed and the upper level subchain numbering continues. An example is shown in Fig. 4.

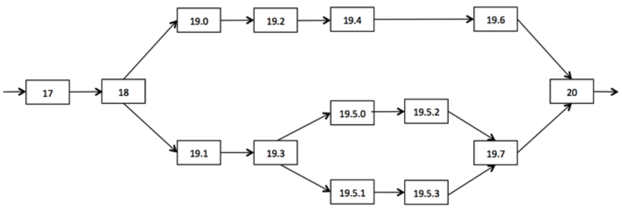


Fig. 4. Block Numbering Example

4.3. Synch Block Placement for Balanced Mining

Without any balancing mechanism, one subchain may progress rapidly and create instability in the P2P mining network. For example, after 4 splits, there will be 16 subchains and the block confirmation time can be 1/16 of 600 seconds, which is 38 seconds. This can cause some instability in the mining network, creating more forks within each subchain [13].

To ensure a balanced mining resource distribution and synchronous progress among the chains, we introduce a concept of synch blocks. A synch block inherits the hash values from all pre-synch blocks in the sibling chain. So until all pre-synch blocks are confirmed, no miner can proceed further. The synch blocks are placed as following. Let *k* be the level of the subchain. The main chain has the level of 0, and the first division creates level 1 subchains, etc. Then at level *k*, synch blocks are placed every 2^k block and the difficulty level is 2^{-k} of the original difficulty. Fig. 5 shows the example of level 1 subchain, where the synch blocks are placed every 2 blocks.

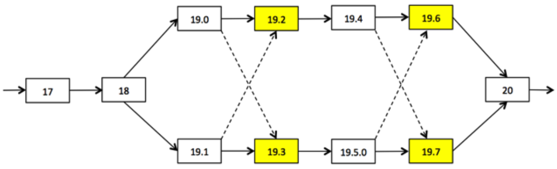


Fig. 5 Synch Blocks

The total amount of work between the synch blocks on Binary blockchain is equivalent to the amount of work for one block in traditional blockchain. Generally,

- # of blocks between synch blocks at level k = 2^k
- Total amount of work between synch blocks = $2^k * 2^{-k} = 1$
- Total amount of reward between synch blocks = $2^k * 2^{-k} = 1$

For example, when there are two subchains, the difficulty level is halved, and the number of blocks between the synch blocks is two including. So the amount of work for two blocks is equivalent to the amount of work for one block in traditional chain.

With this scheme, even if all miners are concentrated on one subchain, the maximum number of blocks they can continuously confirm is equivalent to the amount of work in one block in a classical blockchain. For example, if there are 4 sub-branches, each block can take 2.5 minutes to mine if all miners work on this sub-chain. These 4 consecutive blocks acts like one regular block. The total amount of reward between synch blocks is also equivalent to the reward for one block in traditional blockchain.

The synchronization must be done at all levels to ensure global balancing for all subchains. For example, in a complete Binary blockchain at level k, the number of subchains is 2^k, and the synch blocks must inherit the hash values from all 2^k sibling blocks. This forces global synchronization across all subchains. Fig. 6 shows an example of global scale synchronization.

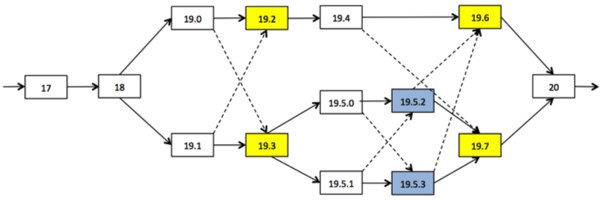


Fig. 6 Global Synchronization

4.4. Autonomous Decision for Split and Merge

In Binary blockchain, the decision to divide or merge is pre-determined by the blockchain itself, not arbitrarily by any individual. The split and merge decision is based on the mining congestion level, and the congestion information can be obtained directly from the blockchain itself. When there is a mining congestion, the transactions must wait longer time to be confirmed. Either a timestamp or the latest block number can be associated with each transaction. Then the average waiting time can be calculated for each block. Then the split and merge rules can be obeyed by all miners as following.

- Split: When the average transaction time in confirmed blocks exceeds a threshold value (e.g., 20 minutes) for predefined periods (e.g., 3 blocks), the Blockchain is split into two.
- Merge: When the average transaction times go below a certain threshold (e.g., 10 minutes) for multiple consecutive blocks for both chains, they are merged. If one of the subchains meets the merge condition, the merge occurs regardless of the transaction load of the other subchain. For simplicity, the merge can occur only at synch blocks.

5. Discussions

5.1. Scalability

Currently Bitcoin mining network can process about 4 to 7 transactions per second. With Binary blockchain, with 10 divisions (2^{10} = 1,024 subchains), the capacity of the mining network can be increased to 3,000 transactions per second, matching the commercial credit card transaction speed (~2,000 per second).

5.2. Cost-Effectiveness

With Binary Blockchain, more transactions can be processed with the same amount of resources. This means the cost per transaction becomes lower. Under mining congestion, users are forced to pay a higher transaction fee to reduce confirmation time, but thanks to the increased capacity, the transaction fees can be kept at the same level.

5.3. DDoS Attack-Resistance

Since Binary blockchain can respond to the transaction load dynamically, the number of subchains is increased automatically during a DDoS period and decrease when the attack is finished. Thus it can effectively cope with a DDoS attack.

6. Performance Evaluation

6.1. Scalability Analysis

In a traditional blockchain, the average mining throughput is given as following.

Mining throughput (=number of transactions / second) = $S_B / S_T / T_B$, where

- S_B = Max size of a block (Currently 1 MB)
- S_T = Average size of each transaction (250 to 500 bytes)
- T_B = Average block conformation period in seconds (600 seconds on average)

With the above typical values, the mining throughput is 3.33. (= 1 MB / 500 Bytes / 600). Multiple proposals are in play to increase the block size. If the block size gets increased, the throughput goes up linearly. For example, with a 4 KB block size, the throughput will be increased to about 13 transactions/sec.

In Binary block chain, the throughput is increased linearly with the number of subchains. For example, with 10 subchains the throughput is increased by 10 times, i.e., 33.3 transactions per second. Note that the number of subchains may not be a power of 2 because each subchain can be split independently.

6.2. Average Confirmation Time

For most Bitcoin users, the ultimate concern is the confirmation time for their transactions, not the mining network throughput. A normal queuing process does not apply because the confirmation is a result of random selection. Different miners receive a different set of transactions, called mempool [3], while transactions propagate throughout the P2P network. In particular, the confirmation time follows a geometric probability distribution. The average confirmation time depends on the overall transaction load in the whole Bitcoin mining network. The probability of being included in the next block for a transaction is N_B/N_T, where

- N_T = Total number of pending transactions in the mining network
- N_B = Number of transactions in each block

Let N_B/N_T be denoted by *p1*. If the number of incoming transactions per block confirmation period is always same as N_B, the total number of pending transactions (N_T) is constant. Then the probability to be included in the *n-th* block (= p_n) for a transaction is,

$$p_n = p_1 * (1 - p_1)^{n-1}$$

In a geometric distribution, the average and variance are given as following.

$$E(n) = \frac{1}{p_1}, \qquad var(n) = \frac{(1 - p_1)}{{p_1}^2}$$

In case of Binary blockchain, the confirmation time is given as follows.

$p_n = (p_1 * N_c) * (1 - p_1 * N_c)^{n-1})$, where

- N_c = Number of subchains
- $\lceil p_1 * N_c \rceil = 1$

The average and variance are given as following.

$$E(n) = \frac{1}{p_1 * N_c}\,, \qquad var(n) = \frac{(1 - p_1 * N_c)}{(p_1 * N_c)^2}$$

For a comparison, the confirmation times in both cases are shown in Table 2 under the following conditions.

- N_T = 10,000
- N_B = 2,000
- N_C = 2
- p_1 = 0.2 (= 2,000 / 10,000) for traditional blockchain, or
  p_1 = 0.4 (= 2,000 * 2 / 10,000) for Binary blockchain

The corresponding statistical values are given in Table 3. We can observe that the conformation time gets reduced greatly by increasing the throughput by twice.

Block period	Traditional blockchain	Binary blockchain with 2 subchains
1	0.200	0.400
2	0.360	0.640
3	0.488	0.784
4	0.590	0.870
5	0.672	0.922
6	0.738	0.953
7	0.790	0.972
8	0.832	0.983
9	0.866	0.990
10	0.893	0.994

Table 2. Probability of confirmation within n-th block

	Traditional blockchain	Binary blockchain with 2 subchains
Average	5	2.5
Variance	20	3.75
Standard Deviation	4.47	1.94

Table 3. Statistical values of confirmation times

6.3. Simulation Results

To test the scalability of the Binary blockchain, we performed simulation under the following conditions.

- Total number of transactions per block = 500
- Block confirmation period = 10 minutes (= 600 seconds)
- Number of block periods = 50 (= 500 minutes)
- Transaction fee = none (not considered)

We generated the transaction as following. First, we generated 500 transactions per block period with the initial transactions of 1,000. In each block, 500 transactions are selected randomly. In this case, there is no backlog and the behavior of the traditional and Binary blockchain was identical. Second, the transactions are generated uniformly at the speed of 1,000 transactions per second. Fig. 6 shows the result.

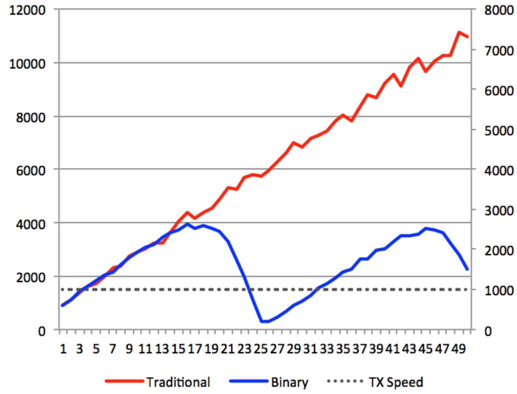


Fig. 6 Response to a Gradual Increase

Since there are 500 transactions not included in a block each period, it creates a gradually increasing mining congestion. The result is an increased average transaction confirmation time due to the growing waiting period. In case of Binary blockchain, when the average confirmation time is over 3,000 seconds continuously for 3 blocks, it divides the blockchain. Reversely, if the average confirmation time is below 1,500 seconds for 3 blocks continuously, it merged the subchains. The traditional blockchain shows gradually increasing average transaction confirmation time. The Binary blockchain shows quick drop in the average confirmation time after a division (around period 17) and consumes most of the backlogged transactions. At the lowest point (period 29), the confirmation time went down to 299 seconds. Then the subchains are merged, thereby having a more consistent average confirmation time within a range.

Third, we simulated a sudden surge of the transaction load such as in DDoS attack. Fig. 7 shows the result. In this case, there was a large amount of incoming transactions (up to 4000 transactions per block period) between the block periods 19 and 25. As expected, the traditional blockchain couldn't handle the transaction load and the average confirmation time kept increasing. In Binary blockchain, the blockchain was divided first when the normal overload was observed (around period 17). Then when the surge hit, it divided again (around period 25) and reduced the confirmation time down to 637 seconds (period 37). Then it merged as the load subsided average and the transaction time went up to the normal range. This results show that Binary blockchain can adjust the capacity to the changing load effectively.

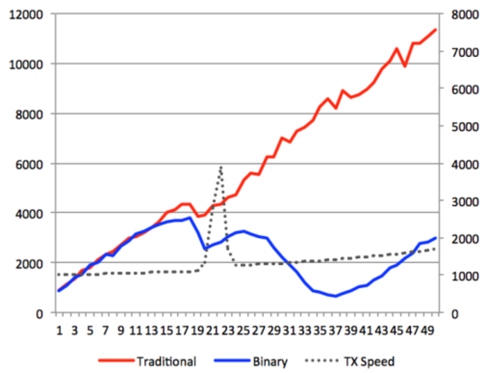


Fig. 7 Response to a Temporary

7. Conclusions

Mining congestion is a serious problem that limits the growth a blockchain-based cryptocurrency. Although many schemes have been proposed to resolve the issue, it is not clear yet if they can scale up to the level of commercial credit card transaction processing speed. In this research, we have proposed a dynamically scalable solution called Binary blockchain. It takes advantage of the simplicity of binary operation on division, merge, difficulty level adjustment, and reward adjustment. To prevent imbalanced mining, it employs a synch block system. The decision to divide or merge is made by the blockchain itself, so every miner can follow the decision unanimously. Binary blockchain can adjust the mining capacity according to the transaction load, thereby providing a more consistent confirmation time regardless of the load. We have tested its performance in simulation and observed that Binary blockchains successfully adjusts the mining speed according to the transaction load. Although the actual parameters, such as the threshold times or the number of consecutive blocks, should be further studied, the experiment demonstrates the validity of the Binary blockchain concept.

References

1. Y. Banjo, “Ethereum won’t scale like you’ve been told.” October 31, 2016, https://medium.com/@yobanjo/ethereum-wont-scale-like-you-ve-been-told-cae445bef539#.x9j5rd2uy.
2. G. D. Battista, V. D. Donato, M. Patrignani, M. Pizzonia, V. Roselli and R. Tamassia, "Bitconeview: visualization of flows in the bitcoin transaction graph," 2015 IEEE Symposium on Visualization for Cyber Security (VizSec), Chicago, IL, 2015, pp. 1-8.
3. Bitcoin Ticker - Charts, “Num TXs held in mempool,” http://charts.bitcointicker.co/#mempooltrans.
4. J. Blocke, “The Network Congestion Problem,” October 16, 2016, https://keepingstock.net/network-congestion-is-problematic-c9d7829ed4ec#.d91t6vk9u.
5. J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll and E. W. Felten, "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies," 2015 IEEE Symposium on Security and Privacy, San Jose, CA, 2015, pp. 104-121.
6. Bravenewcoin.com, “Bitcoin Block Size Debate Survey,” September 2015, http://bravenewcoin.com/assets/Blockchain-Scalability-Survey-2015/BNC-The-Blockchain-Scalability-Survey-2015.pdf.
7. V. Buterin, “Scalability, Part 3: On Metacoin History and Multichain,” November 13, 2014, https://blog.ethereum.org/2014/11/13/scalability-part-3-metacoin-history-multichain/.
8. Vitalik Buterin, “Uncle Rate and Transaction Fee Anaysis”, https://blog.ethereum.org/2016/10/31/uncle-rate-transaction-fee-analysis/, Oct. 31, 2016.
9. M. Carlsten, H. Kalodner, S. M. Weinberg, and A. Narayanan, “On the Instability of Bitcoin Without the Block Reward,” Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS), Vienna, Austria, October, 2016, pp. 154-167.
10. A. Chernyakhovsky, “Bitcoin Scalability: An Outside Perspective,” September 28, 2015, https://medium.com/mit-media-lab-digital-currency-initiative/bitcoin-scalability-an-outside-perspective-dd7fde962220#.1i44lqxas.
11. K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels,A. Kosba, A. Miller, P. Saxena, E. Shi, E. G. Sirer,D. Song, and R. Wattenhofer, “On scaling decentralized blockchains,” 3rd Workshop on Bitcoin Research (BIT-COIN), Barbados, February 2016.
12. C. Decker and R. Wattenhofer, "Information propagation in the Bitcoin network," IEEE P2P 2013 Proceedings, Trento, 2013, pp. 1-10.
13. I. Eyal, “The miner’s dilemma,” 2015 IEEE Symposium on Security and Privacy, San Jose, CA, pp. 89–103. 2015.
14. I. Eyal and E. G. Sirer, “Bitcoin-NG: A Secure, Faster, Better Blockchain,” October 14, 2015,

http://hackingdistributed.com/2015/10/14/bitcoin-ng/.

15. I. Eyal, A. Efe Gencer, E. Gün Sirer, R. van Renesse, "Bitcoin-NG: A Scalable Blockchain Protocol," 13th USENIX Symposium on Networked Systems Design and Implementation, Santa Clara, CA, Mar. 2016.
16. D. Gilbert, "Blockchain Complaints Hit Record Level As Bitcoin Transaction Times Grow And Fees Rise," March 8, 2016, http://www.ibtimes.com/blockchain-complaints-hit-record-level-bitcoin-transaction-times-grow-fees-rise-2332196.
17. G. Greenspan, "MultiChain Private Blockchain — White Paper," Coin Sciences Ltd., http://www.multichain.com/download/MultiChain-White-Paper.pdf.
18. P. Jovanovic, "ByzCoin: Securely Scaling Blockchains," August 4, 2016, http://hackingdistributed.com/2016/08/04/byzcoin/.
19. G. O. Karame, "On the Security and Scalability of Bitcoin's Blockchain," Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security (CCS), Vienna, Austria, October, 2016, pp. 1861-1862.
20. E. K. Kogias, P. Jovanovic, N. Gailly, I. Khoffi, L. Gasser and B. Ford, "Enhancing Bitcoin Security and Performance with Strong Consistency via Collective Signing", 25th USENIX Security Symposium, August 2016, Austin, TX
21. T. McConaghy, "Blockchain Scalability Part I – The Problem," February 14, 2015, http://trent.st/blog/2015/2/14/blockchain-scalability-part-i-the-problem.html.
22. J. Poon and T. Dryja, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments," Technical Report, https://lightning.network/lightning-network-paper.pdf, Jan. 2016, Draft Version 0.5.9.2.
23. A. Quentson, "Cornell Study Recommends 4MB Blocksize for Bitcoin," March 31, 2016, https://www.cryptocoinsnews.com/cornell-study-recommends-4mb-blocksize-bitcoin/.
24. Pater R Rizun, "A Transaction Fee Market Exists Without a Block Size Limit", https://www.bitcoinunlimited.info/resources/feemarket.pdf, Aug 5, 2015.
25. Greg Sanders, "Sidechains, Treechains, the TL;DR, welcome to join discussion." Jine 13, 2014, https://blog.greenaddress.it/2014/06/13/sidechains-treechains-the-tldr/.
26. K. Torpey, "6 Possible Solutions for Bitcoin Scalability," June 30, 2015, https://www.coingecko.com/buzz/six-possible-solutions-for-bitcoin-scalability.
27. F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," in IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2084-2123, third quarter 2016.
28. M. Vukolic, "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication," In Open Problems in Network Security - IFIP WG 11.4 International Workshop, iNetSec 2015, Zurich, Switzerland, October, 2015, Revised Selected Papers, pages 112–125, 2015.