Why I support Big Block Bitcoin

Kazuki Sugiyama
Electronic-Mechanical Engineering Course,
Department of Mechanical and Aerospace Engineering,
School of Engineering, Nagoya University
235711131719k@gmail.com

1. Introduction

Bitcoin is a peer-to-peer electronic cash system([1]). It's the first crypto currency. Crypto currency is the decentralized digital currency and realized with "Cryptography", "Game Theory" and the unique database called "Blockchain."

2. How to realize dicentralized currency

Bitcoin is like email, we can get Bitcoin address and send or recieve Bitcoin using an address. One person can have many Bitcoin addresses and we can't know who has the Bitcoin address. When we send Bitcoin, we make the transaction(which address send, which address recieve, the number of sending Bitcoin, have sending authority, etc.) and is broadcasted to Bitcoin server called nodes in the world. Nodes are distributed all over the world managed by various people, organization and company. All nodes synchronize together and save the Bitcoin database called "Bitcoin Blockchain." Bitcoin Blockchain is a sequence of blocks, and block contain Bitcoin trasaction data every about 10 minutes(fig1). So Bitcoin Blockchain saves all bitcoin transaction data which is verified. Bitcoin nodes collect justifiable transaction as a block about every 10 minutes.

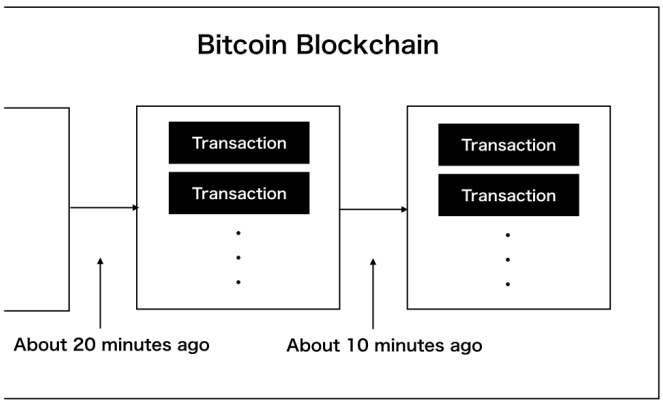

Fig. 1. Bitcoin Blockchain

Bitcoin is a decentralized system, which means a person or organization who control Bitcoin doesn't exist. Then How can nodes verify transaction and who add a block to Bitcoin Blockchain every about 10 minutes? The Bitcoin mining system called "Proof of Work" solves the problems. When nodes add a block to Bitcoin Blockchain, nodes have to solve the simple(not easy) math puzzle using a computer. In other words, nodes who can first solve the problem have the authority for adding the block. If we want to change the history of Bitcoin transaction, we have to solve the enormous math problem. It's the source of Bitcoin security. The activity for solving the problem to add block is called mining, and nodes who do mining are called miners. Because miners use electricity for mining, a miner who add a block gets a mining reward. The mining reward consists of two factors, block reward and the sum of transaction fee in the block. Now, block reward is 12.5 Bitcoin and it's only the generation of Bitcoin. Therefore, Bitcoin miners have a lot of Bitcoin. If miners have enormous machine power for mining, they can almost control Bitcoin, but they don't do that. If they attack Bitcoin such as change transaction history, Bitcoin value becomes low and miner suffer a loss compared to not attacking because they have a lot of Bitcoin. Proof of Work manage the incentive of miners using Game Theory. Finally Bitcoin achieve the decentralized currency.

3. Trilemma of crypto currency

Crypto currency is not mature technology and it has trilemma([2]) which means that crypto currency can achieve two of below three factor, but can't achieve all.

- **Decentralization** : distribution of nodes which run crypto currency software in the world
- **Scalability** : the number of transactions per second it can verify
- **Security** : being secure against attackers

Classical crypto currency(Bitcoin, Ethereum, etc.) achieve decentralization and security, but sacrifices scalability. Actually, BitcoinCore(BTC) can verify only about 5 transactions per second. Recent crypto currency(EOS, Tezos, etc.) achieve Scalability and Security, but sacrifice decentralization. Actually in EOS, only 21 nodes can verify EOS transactions and add blocks to blockchain(table1). So, a lot of crypto currency has been developed to bleak the trilemma.

4. Scalability of Bitcoin

Of course, Bitcoin has been also developed to improve the scalability. Now, there are below two major scaling options for Bitcoin. Two Bitcoin, BitcoinCash(BCH) and BitcoinCore(BTC), implemented individually.

Table 1. Trilemma of crypto currency

	classical(Bitcoin, Ethereum)	recent(EOS, Tezos)
Decentralization	◯	×
Scalability	×	◯
Security	◯	◯

- **Big Block(called *on chain scaling*)** :Implemetation in BitcoinCash(BCH)
- **Lightning Network(called *off chain scaling*)** :Implemetation in BitcoinCore(BTC)

Big Block is the simplest and easiest method for scaling Bitcoin. The reason of about 5 transactions per second is that the capacity of the Bitcoin block is about 1 MB. All Bitcoin transactions in the world in about 10 minutes is limited to only about 1 MB. It's too small! Let's change the block size more bigger. That's the Big Block idea. Of course, some demerit exists in it's idea. Too Big Block such as 100 MB may make Bitcoin Blockchain more centralized. Big Block can contain a lot of transactions, which means blockchain size nodes have to maintain is big. And nodes have to spread a lot of transaction data, so nodes have to have good network ability. That may reduce the number of nodes.

Lightning Network is the idea that we don't have to save all transaction data, but we have to save only the digest for some period. For example, Alice goes to the cafe every day, and pays with Bitcoin. Conventionally we have to save the payment transaction every day, but Lightning Network saves the digest of the transaction once some period(such as a week) without trusting the others(fig2). If Bob also pays the cafe with Lightning Network, Alice can send Bitcoin to Bob with Lightning Network, and vice versa. But realizing Lightning Network is very difficult technically. And Lightning Network may also make Bitcoin more centralized because the broker(the cafe of the example) of Lightning Network has the power.

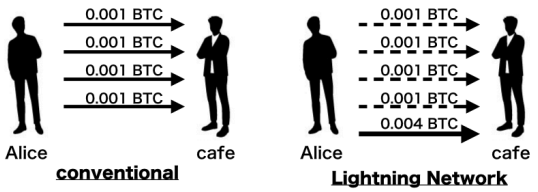

Fig. 2. example of Lightning Network

Table 2. comparison of Big Block and Lightning Network

	merit	demerit
Big Block	simple, easy	centralized
Lightning Network	scale on small block	difficult, centralized

5. Bitcoin System is based on Big Block

Bitcoin System is based on Big Block and can't avoid Big Block because Bitcoin block reward reduce by half in about four years and the sum of Bitcoin has the limit(21,000,000 Bitcoin). Bitcoin imitates gold to make people think Bitcoin which is the first crypto currency is valuable. So, finally the reward Bitcoin miner can get is just the transaction fee. Now, mining reward(Block reward + transaction fee) is almost all Block reward. If transaction fee in a block is left, Bitcoin miner can't afford the mining cost and Bitcoin becomes low security system. So we must raise Bitcoin block size, transactions which are contained in the block and sum of the transaction fee Bitcoin miner can get.

6. Conclusion

Because of the limit of the Bitcoin amount and the mining system, we should raise block size and try to solve scalability problem by Big Block. We can't avoid Big Block Bitcoin. If we avoid that, Bitcoin must collapse.

References

1. Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," (https://bitcoin.org/bitcoin.pdf)
2. Vitalik Buterin, *Sharding FAQs* (https://github.com/ethereum/wiki/wiki/Sharding-FAQsthis-sounds-like-theres-some-kind-of-scalability-trilemma-at-play-what-is-this-trilemma-and-can-we-break-through-it).
3. Joseph Poon and Thaddeus Dryja, "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments," (https://lightning.network/lightning-network-paper.pdf)