Bitcoin Reading Report

Weiting Li

March 2022

1 Summary

In this paper, Satoshi Nakamoto, the anonymous author, introduce to us a possible solution to the problems with transactions that go through traditional financial institutions: A decentralized electronic payment system based on cryptographic proof of work instead of trust to centralized systems like banks, credit card company. This system is able to make non-reversible payments which makes fraud impossible because of the amount of computational power to make fraud happen. It uses a peer to peer distributed timestamp server : the Blockchain to record transactions in a chronological order. It is secure as long as honest computer nodes have more computational power than the fraudulent party.

2 Problem

In the bitcoin whitepaper, the problem the author wants to solve is the double spending problem. Because if digital signatures for an electronic cash still require a trusted third party, there is a huge loss of the benefits of using electronic currency.
And bitcoin will have the ability to tackle some problems that earlier cyrtocurrency like b-money fail at. It is a distributed system instead of using a centralized ledger to verify payments. Thus, it avoided the single point of failure: it is impossible for hacker to attack just one central node to paralyze the system and it does not have the con of breaking down due to technical issue.

3 Importance

There are several advantages of using a peer to peer electronic cash system. First and foremost, traditional banks and credit card companies are stable at the moment but it has a lot of defects. And bitcoin is invented to be the perfect solution to these. Here is a list I summarized from the paper:

1. **Completely non-reversible transactions are not possible because of the mediating role of these financial institutes.** This leads to the high transaction cost. And as a result, small transactions that may be less than the transaction fee is not practical. For example, spending 10 cents for an access to an article or a video.
2. **Loss of ability to make non-reversible payments for non-reversible work** such as viewing a vid. This causes that sellers have to take more actions like gathering more information to avoid fraud and gain from their work. This leads to privacy issue nowadays. And a certain amount of fraud is still unavoidable.

4 Technical challenges

To solve the double spending problem stated above, here are two significant steps that need to happen:

- **Be aware of all transactions but avoid central authority like a bank.**
- **A system that a majority of nodes to agree on a transaction's credibility.**

- **A way to decide between two transactions that spending the same coin, which comes first.**

5 Key Insights Contribution

Satoshi proposed a better way to build up electronic cash system that is a purely peer to peer, easy to implement, stable and trustworthy, and also supports non-reversible payments which traditional financial institution usually do not. Bitcoin is his perfect solution to tackle all of the technical issues above.

To solve the double-spending problem, which is the most troublesome issue exist in any electronic coin without trusted third parties, Satoshi suggested bitcoin will let every node on the network to see the public transaction record while these transactions are made anonymous to protect user's privacy. For example, when A made a payment(e.g. dinner share) to B, A will spread this information public to all participants on the peer to peer network. This leads to another question: because there is nobody playing the mediator role here, how do we know this transaction is valid and only?

So he suggested adding a feature of timestamp keeping. Every **Block** (a bunch of transactions stacking together) will have a timestamp. Bitcoin uses this timestamp and the digital signature to produce a unique hash value that is not possible to reverse-engineer. This hash value is closely related to the proof of work system in bitcoin. For every block in the network to be valid, nodes will try to random guess a 256 binary value that has the required zero bits. And when this is done, the timestamp is fixed and the miner who found this number will get a reward for his work: the computation power used and made public so that everyone on the network knows. With this novel structure, it is almost impossible for attackers to tamper with the blocks because when one block is changed, all the block after it has to recalculate the hashes to make this action valid. This is a astronomical number of "random guesses" and a perfect mechanism to protect the transaction's integrity unless attackers have more computation power than all the honest nodes on the network. This reward mechanism also helps protect the network because it is just not worthy to tamper rather than just play by the rule book (be an honest notetaker).

In addition, his paper also touches on some aspects like method to free the disk space and way to simplify payment verification.

Personally, I found Bitcoin's success today unbelievable as a crytocurrency watcher. However, now I think Bitcoin is so prosperous today due to this completeness of this whitepaper.

6 Strength/Weakness

Strength:

1. Bitcoin is the first successful trustless, **globally well known** electronic currency. Its users spread the whole world and it is already changing people's view towards crytocurrencies all over the world.
2. It resolves many issues that traditional financial authorities have such as privacy, high transaction fees, low efficiency, corruption, single point of failure, fraud etc..
3. It is decentralized, limited-supply, not worthy to tamper with, saves the amount of efforts on trust issue, censorship-free, transparent, permissionless. All of these properties produces this irreplicable of bitcoin.

Weakness:

The paper did not touch on issues like:

1. Although it has a maximum of 21 million coins, Satoshi did not recognize that it is almost infinitely divisionable.
2. Furthermore, what is the foundation of the value of bitcoin? Traditional currency usually have a standard. For instance, U.S dollar is correlated with the price of petroleum. The idea right now about what gives Bitcoin value is the cost of the computations to bookkeep the records on individual PCs. What if one day computation power is extremely cheap or some party owns a super computer like a quantum computer?

3. Though bitcoin is comparably trustless, Satoshi probably did not think about that one day other crytocurrencies would surge and a considerable amount of them turns out to be scams. Although this is not directly related to Bitcoin itself, it could leads to distrust from people towards Bitcoin. This would put up a question mark on how far Bitcoin can go. Will it eventually replace all the currencies we have today?

7 Personal intake

From this whitepaper of Bitcoin, I get to know about details of bitcoins like what is the difference between Bitcoin and earlier electronic coins, what makes it special, why it succeed etc.. As a normal human, a buyer of crytocurrency, an optimist who truly believe that Bitcoin has the potential to change human kind that Bitcoin's success will bring us the revolution of currency, this whitepaper gives me a tour on the details of Bitcoin's invention in the very beginning. It is truly genius in my opinion even after reading the paper. However, I am disappointed that this paper did not solve some of the questions I have towards Bitcoin: what makes Bitcoin valuable? Why should people trust it over traditional currency? I hope some genius in the latter days can give me answers to these doubts in the future.