Ozan Cinci

2448223

HW2

Q1)

In traditional payment systems, let's say someone goes to a shop then s/he pays with his/her credit card. How does shop owner accepts payment with credit card? Because the owner trusts the bank that gives this credit card. So, how does the bank trust customer? Because they have enough information to identify customer. This system works and depends on trust. To ensure trust, both customer and shop owner give more information than needed. In this case, the bank is the third-party organization. Normally, the bank has nothing to do with shopping, but we must trust someone to ensure that payment is done in safe way. But can we eliminate the third part trust factor and do the safe transition without needing third party organization so that we do not have to provide our private information to someone else? This paper introduces an idea about peer-to-peer electronic cash transition that eliminates third party organization in a safe way without providing private information more than necessary.

Of course, this problem can be addressed by using cash money. But using cash money all the time is not applicable. Instead of a system that based on trust, bitcoin establishes a system based on cryptographic proof that any two parties can transact directly without trusting a third party. Also, Transactions are completely irreversible so there is no possibility for fraud using double spending. The system security based on one thing; the CPU power of honest nodes must be more than CPU power of attackers' nodes. To summarize previous two paragraphs, bitcoin proposes a solution that prevents double spending and removes third party trust.

In the bank system, we trust to the bank to ensure that no one double spent their money. However, in bitcoin Satoshi want to eliminate third-party organizations, then there must be a solution to prevent double spending without third-party organizations. Satoshi come up with an idea and it is that all the transactions must be publicly announced. There must be a single history about transactions' orders that participants agree. The way order of transactions agreed is that majority of nodes agreed on a transaction arrived before the other one. So, there is a public transaction history, and every node can check if a current bitcoin is spent before, then denies or approves current transaction based on public transaction history. Because the only reasonable way to ensure a bitcoin used in a transaction before is to access and scan all the transactions by now.

To expand what Satoshi means by arriving first, he introduces Timestamp Server. When a bitcoin is transferred, it is hashed by using the hash data from previous blocks. The timestamp is a proof of that the data is validated at the time. By doing this, each block is reinforcing previous

timestamps via generating a chain. So, how to ensure that a chain is the legitimate one? Satoshi introduces proof-of-work concept. Using proof-of-work we can easily verify completed computation while computation itself requires exponential time. Since it requires hash value from previous block, to alter a block, all the blocks coming after it also must be altered, and it requires lots of CPU workload so that all the honest nodes can easily determine longest and the accepted chain using power of majority. To alter a block, attackers must overpower honest nodes while honest nodes adding new accepted blocks.

So why to stay hones and try to extend longest chain? Because every coin supply contributed by miners rewards the miner. So, people are willing to stay honest and mine new coins. While mining new coins, longest chain becomes cumulatively longer. While becoming longer, only condition a block to be accepted by nodes is that all the transactions it contains are valid and not double spent, and nodes are able to check it since all transactions are publicly announced. The way nodes accept a block is working on creating the next block based on previously accepted block. Even if a transaction broadcast does not reach all nodes, reaching out many nodes is enough. As Satoshi mentioned, staying honest is more profitable than breaking rules.

There may be multiple inputs and outputs for transactions since it would not wise to make a separate transaction for every cent. This system works for transactions of small amounts.

A block contains hash value of transactions, but it does not need to store all the transactions' information to verification. To save some space, blocks store hashes of transactions in a structure called Merkle Tree. Transactions' hash values are hashed together again and again until we have Merkel Tree root, and it is enough information to be stored. Moreover, to verify payments we do not need a full network node. Instead, block headers of the longest chain and the Merkle branch linking the transaction to the block it is timestamped is enough to verify.

Although all transactions are announced publicly, there are no names attached to wallet addresses. Everyone can see that someone sends an amount of money to other one but there is no name or address attachment to anyone unless the one who makes transaction reveals his/her wallet on consent.

Q2)

- While Satoshi tries to implement pseudo anonymity, it may not be possible all the time. Since bitcoin's price increased, some countries started to regulate new laws for identity detection and declaration to prevent fraud and wallet theft.

- The main purpose of the bitcoin was creating transaction channel (electronic cash payment system) between two organizations, but it has evolved as some kind of investment tool.
- Satoshi states bitcoin as peer-to-peer transaction without going through third party financial organizations, but today many users use centralized third-party organizations' products to trade, exchange bitcoin and store their wallets.
- Satoshi visions that bitcoin may be used for everyday transactions even if small sized ones with zero or low transaction fees, but this is impractical today. Increase in the value of bitcoin and some scalability problems makes transactions fees relatively high. So, doing everyday transaction with bitcoin has become impractical. It has evolved more like an investment tool.
- The user pool has become larger and larger, the number of miners has increased. As a result, electric consumption and costs have increased. It has created environmental problems leading to questions about miners' effects on environment. Then causes some countries to make regulations about mining.
- Satoshi states that it was designed to be a decentralized system. He couldn't predict that there will be big investors who invest big amounts of money into dedicated hardware to dominate the CPU power on pool. As a result, the mining process has inevitably become less decentralized.