**Reading summary of Shaoyu Li**

Shaoyu Li

shaoyuli@vt.edu

Virginia Tech

Falls Church, Virginia, USA

**1 What is the problem the paper is trying to solve?**

The paper is trying to offer a system that does not need trust. The only thing that the system considers is cryptography technology, which can help some parties send information or conduct transactions without the third-party service or management. The system can make sure that the data in the system is computationally hard to modify or change. The system can run smoothly if the CPU power of the honest nodes is larger than malicious nodes.

**2 Why is the problem important to solve?**

In our real world, we rely on some centralized systems to conduct transactions, which means that we need to trust some third parties. However, the model has some problems. For example, it is hard for third parties to offer the service that data cannot be modified. Therefore, the third parties need to maintain the system to keep the data secure. It needs to cost lots of money and resources. In addition, the system has some limitations like collecting more information of customers than real needs. Customers do not want to trust the service provider.

**3 What are the technical challenges for solving the problem?**

1. As for one transaction, the sender needs to use something to ensure that the transaction is from him and he owns enough money to pay. Also, he needs to identify the receivers who can control the money.
2. Because digital transactions are really easy for others to copy, the system needs to avoid double-spending attacks.
3. How does the system store the information of transactions and how does it ensure that data will not be modified?
4. A consensus is needed to let all nodes in this system believe that each transaction in the system is valid.

1. How to store the transaction information for others to do the easy check?

**4 How does the paper solve the problem? Key insights? Technical contributions?**

The system uses asymmetric encryption technology to create a pair of private keys and public keys for each address. If one address wants to initialize a transaction, he can use his private key to give a digital signature of the transaction information. Others can verify his transaction by using his public key. The other significant point is to ensure that the address has enough money to pay. Therefore, the money used in the new transaction needs to be linked with the previous transaction where the sender got the money.

The system uses a timestamp server to ensure that the transaction is here at a specific timestamp to avoid double-spending. The system uses different blocks to store different transactions at different time stamps. The new block needs to contain the hash value of the previous one to show that the new block’s timestamp is newer than the previous one.

The system uses proof-of-work to expand blocks to contain more transactions. It means that the nodes that have more CPU power can decide which transactions can be stored in the system. In each block, there are two parts, block header, and block body. The proof-of-work needs to calculate the result of the nonce in the block header so that the hash value of the block header is on a target scale. The nonce can only be tried one by one, which means that there is not an easier method to get the result. Of course, the difficulty can be modified according to the time to calculate the result of the previous blocks’ nonce. To incentive more nodes to take part in the calculation activity, there are some rewards when a miner creates a new block successfully. The miner can get some bitcoins from the coinbase transaction, which does not have the input data.

As for transactions’ storage, the system uses the block body in one block to store all the transactions selected by the miner of this block. All nodes can't store so much data in their disk. Therefore, the system can build one Merkle tree in each block to store the information of all transactions in this block. The block header store the Merkle hash root of the tree. Some light nodes only need to store the information of all block headers, without the block bodies. It is convenient for others to verify one transaction because they only need to get the transaction hash and calculate its root, which can be compared with the root in the block header.

When the new block is broadcast on the network, others will verify the block when they receive the block. If the block is valid, honest miners will stop their previous work and mine the next block links to the broadcast block. Sometimes there is a forked chain because of some reasons like the broadcast delay or malicious activity. The honest miner will choose the correct chain according to the order of the received block and mine in the correct chain. Finally, the longest chain will be the main chain and other chains will be discarded. That is the consensus.

**5 What are the strengths and weak- nesses of the paper? How do you like it?**

**Strengths**: It is really hard to modify the information stored in the blockchain. Each node has its local record so that even if some nodes change their local information, it will not influence others. We do not need to rely on the third-party or trust anyone, because of the use of cryptography technology. The double-spending attack is hard to initialize because it needs lots of computing power.

**Weaknesses**: The system needs each full node to offer so large space to store all the transaction information and other data. Normal computers cannot do that. In addition, lots of power will be utilized to calculate the nonce, so that it is nearly impossible for a normal computer to get the result. And the calculation will waste lots of power which may cause serious problems in our real world. Nowadays, there are lots of large mining pools to conduct the calculation, which is centralized in a way and we do not want to see that.

**6 What have you learned after rea- ding this paper?**

The bitcoin system offers us a new design if we want to store something but do not want to trust others. We can not only use the bitcoin systems to store information but use our blockchain to run the system and store what we want to store or share. The data will not be modified in the blockchain. We can also use blockchain to write code like contracts, which will not be modified and we can only conduct the contracts because we cannot change the state of the code without changing its content.