Deniz Aytemiz

CS 5594: Blockchain Technologies- Paper Summary 1

Question 1: What is the problem paper trying to solve?

Answer: This paper is the white paper of bitcoin. The main problem it attempts to solve is removing the requirement of trusted third parties in the process of cash transaction between two parties in the non-physical environment, especially for the issue of double-spending. Trusted third parties such as banks, put extra cost on the transaction due to its services as being mediator. They make the transaction possibly reversible and can put limits or rules based on the transaction which makes them somewhat impractical and costly. Therefore the paper states that it suggests a safe (in terms of confidentiality and privacy), efficient and no human factor involved peer to peer electronic payment system that would eliminate the problems trusted third parties bring.

Question 2: Why is the problem important to solve?

Answer: The problem is very important especially in current days since the majority of commerce is being processed online. Physical transactions are no longer as widespread as they used to be. Online commerce has its own benefits yet they also bring many concerns along with them such as fraud and double-spending. Buyers and sellers need a third party they can trust in the process of transactions and that also brings issues with itself as extra cost and privacy concerns. These third parties can also go bankrupt or get hacked and the whole system depends on them. Therefore there needs a better system that would bring more trust and efficiency in this process.

Question 3: What are technical challenges for solving this problem?

Answer: There is the double-spending problem. In order to avoid double-spending each transaction should be checked. Achieving this without a central authority is challenging. In addition there is the problem of replicating/ stealing someone's digital signature. People should be able to sign and verify the transactions and these should be observed by the public yet they need their signatures to be just for themselves to avoid fraud. These privacy concerns are tackled with cryptographic methods as hash functions and asymmetric encryptions.

Question 4: How does the paper solve the problem? Key insights? Technical contributions?
Answer: In the proposed model, transactions are publicly announced and all participants in the network have a copy of the transaction history. This makes it possible for everyone to agree on a single transaction history. If there are different versions of a transaction history, the one that has the most computational work (the longest chain) is selected. List of transactions, proof of work and the hash of the previous block are held in the block. Since each block is inherently dependent on the previous one, the whole blockchain becomes temper proof. In order to alter the content of a block you have to alter all the previous blocks since the hash will change, which is infeasible. The people doing the proof of work (solving the puzzle) are rewarded with assets so they are encouraged to work truthfully. And the payee can feel more trust since the transaction history is seen and verified by majority. Once a transaction is buried under enough blocks, the previous transactions can be discarded to save space without breaking the hash of the current block.
Each block hash is timestamped and each timestamp has the hash of the previous timestamp. These are broadcast publicly for everyone to see. The transactions themselves are digitally signed and verified by the owners leveraging the asymmetric encryption.

Question 5: What are the strengths and weaknesses of the paper? How do you like it?
Answer: The strengths are privacy, confidentiality and decentralization. This technology allows users to make asset transactions without relying on a central authority, precludes double spending and it is very difficult to tamper with the transaction history due to its chain nature. Considering the weaknesses, the block creation time can take significant time and CPU power due to the proof of work. This can cause problems since there are many transactions taking place at the same time and the system should be able to quickly and efficiently put them into process. In addition, since the blockchain mainly relies on the CPU power even though it is not very likely it still is vulnerable to 51% attack in which an attacker gets the majority of the CPU power in the network and is able to cause fraud.

Question 6: What have you learned after reading this?
Answer: I have learned the main technical components underlying the idea of blockchain. I have learned how the owner signs and verifies transactions and how the system is designed for

encouraging the participants to be honest. I also have learned how the majority decides on the true blockchain and avoids fraudulent ones.