Lecture 5 – Bitcoin in research overview summary – Tien Dat Le

Bitcoin emerged as one of the most successful cryptocurrency that has been widely adopted since 2019. Although it is proved to work in practice, there are many literatures recently pointed out hidden-but-important properties of the system, discovered attacks, theoretically scalability limit of the system, proposed alternatives solutions that might assist to solve these challenges.

Since Bitcoin is one of the first system that introduced incentivize reward for miner to solve the consensus problem that in normal byzantine settings is unsolvable. It has to depends on an assumption that miners will follow game theory strategy, hence posing a research problem in proving the stability of incentive and compiling. It is proved that simple majority compliance may not ensure fairness, as of selfish mining attack. However, majority compliance is an equilibrium with perfect information, thus, implied that Bitcoin is weakly stable. Moreover, with a majority miner, stability is not guaranteed and also in case miners can collude. Stability is also not known when the mining reward vanish.

The theoretical limitation of Bitcoin system is also measured and analyzed some of its characteristic, namely: maximum throughput, latency, boostrap time, cost per confirmed transaction. The research has proved that given the current overlay network and average block time is 10 minutes, the blocksize should not exceed 4MB, correspond to a throughput of at most 27 transaction per second. For the latency limit, to retain at least 90% effective throughput and fully utilize the bandwidth of the network, the block interval should not be significantly smaller than 12s.

There are also many useful modification is suggested for Bitcoin. Firstly, it is suggested that for Bitcoin light client, it can used simplified payment verification so that it does not need to store the entire blockchain, yet it still can validate the correctness of transaction. Key management in client is also important point to modify such as: split control, password-protected wallet, offline storage and hardware storage. There are also research on changing parameters to optimize bitcoin performance, finding new approach for proof of work, namely proof of stake, consortium consensus or sharding. Alternative computational puzzles such as ASIC-puzzles, useful puzzles, and nonoutsourceable puzzles is also studied for strengthen the mining work. There are also research about anonymity and privacy that proposing mixing protocol and unlinkable altcoins such as Zerocoin and Zerocash. The extended application of Bitcoin also discussed such as: secure timestamping, digital tokens such as coloured coins and overlay protocol such as master coins.