Summary of Bitcoin in research

February 20, 2018

# 1 Bitcoin under the hood

This is an article of an magazine. It highlights in three aspects.

One is the distributed ledger of transactions that is synchronised between all nodes. The challenge is to ensure nodes agree on the contents of this ledger.

The protocol faces many challenges, including the privacy of users, scalability and robustness of the network, decentralized mining and incentives of mining.

The last one is to show the continuous innovations are slow, however, Bitcoin may become a meaningful force in the global money transmission market.

# 2 SoK: research perspectives and challenges for Bitcoin and cryptocurrencies

This paper gives an overview of Bitcoin and cryptocurrencies from the research perspectives and challenges. It first introduces the history of Bitcoin and explain the reason why it is worth to be researched. Then it presents the techniques used in the Bitcoin, including transaction, consensus, mining and network. The stability of Bitcoin is analysed. It includes stability of transaction validity rules, the consensus protocol, mining pools and peer-to-peer layer. The security issue is also discussed, especially the key management. To improve the Bitcoin, many modifications are given, e.g., for updating the Bitcoin, soft fork and hard fork are applied. For the scalability, it introduces the way to change parameters. In addition, different computational puzzles are proposed. Before describing the extension of Bitcoin's functionality, anonymity and privacy are discussed.

# 3 On scaling decentralized blockchains

This paper analyses the current peer-to-peer overlay network over cryptocurrencies, specially emphasising on the scalability of the network.

Compared with the Visa credit card payment reaching 56000 transactions per second, the Bitcoin only achieves 7 transactions per second. An effective way for scaling is by parameter tuning, e.g., increasing the block size. However, due to the fundamental limit of

the throughput and latency, the block size should not exceed 4 MB, based on the current average block interval, 10 minutes and the block interval should be larger than 12s if existing overlay network is given. There are two ways to improve the network plane. One is to avoid transferring each transaction twice and another one is to use a dedicated, centralised, high-speed relay network.

For the consensus plane, in addition to the proof-of-work, proof of stake and consortium consensus are candidates. Moreover, sharding techniques and delegation of trust and a hierarchy of sidechains are proposed for scaling.

The storage plane functions as a global memory that stores and provides availability for authenticated data produced by the consensus plane. The storage plane in Bitcoin only accepts *write* and does not support *delete*.

The view plane is used to show the state of the full ledger, e.g., UTXO set, including technology of view replication and outsourcing view via cryptography.

Side Plane is the off-the-main-chain and it can be implemented to realise different functionalities.

The problem of proposing a proper measurement techniques for decentralised system is still open and considering robustness, scalability and so on, to propose a formally provable security is a non-trivial challenge.