ADVANCED BLOCKCHAIN STORAGE

Xiaojie Zhu

April 24, 2018

1 Summary

The traditional bitcoin network needs almost ten minutes to confirm a transaction. To enhance this process, many alternative consensus protocols are proposed. However, the proposed alternative consensus protocols are not scalable.

The paper, *a secure sharding protocol for open blockchains*, proposes a distributed agreement protocol for permission-less blockchains called ELASTICO. By securely partitioning the mining network, the ELASTICO achieves scaling transaction rate linearly with available computational for mining and based on the parameter setting it is able to tolerate one-fourth of the computation power hold by the byzantine adversary. Specifically, the ELASTICO consists of five parts, identity establishment and committee formation, overlay setup for committees, intra-committee consensus, final consensus broadcast, and epoch randomness generation.

The paper, *IPFS-content addressed, versioned, P2P file system*, proposes a peer-to-peer distributed file system. It applies Kademlia distributed hash table to coordinate and maintain metadata. BitTorrent is utlized to exchange blocks and Git is used to control versions of systems. In addition, self-certified filesystem is applied to define the name system. Specifically, the IPFS consists of seven parts, identities, network, routing, exchange, objects, files, and naming. The identity is generated by the cryptographic hash of a public-key, accompanying with the S/Kademlia's static crypto puzzle. The IPFS can use any network but features at transport, reliability, connectivity, integrity, and authenticity. The routing mechanism needs to realise peer and object searching. The BitSwap protocol is proposed to realise block exchange between peers. Object mercle directed acyclic graph is built, where links between objects are cryptographic hashes of the targets. There are three file objects, blob, list, and tree. The IPNS is designed to build naming space and mutable state. The ambitions vision of the IPFS is to push the web to new horizons.