区块链作业九

SA20225085 朱志儒

1. How would you implement Zero-Knowledge Proof in Ethereum and Hyperledger?

I will implement zk-SNARKs as part of the Byzantium upgrade to allow for transactions to be verified while protecting user and transaction privacy.

In Hyperledger Fabric, I will use identity mixer to implement anonymous client authentication. I will realize privacy-protected asset exchange through Zero-Knowledge Asset Transfer(ZKAT).

1. What are zk-SNARKs?

Zk-Snarks was introduced in 2012 by Nir Bitansky, Ran Canetti, Alessandro Chiesa & Eran Tromer and describes a special variation of the zero-knowledge technique. Zk-Snarks introduce a number of innovations that render them usable in blockchains. Most importantly, zk-Snarks reduce the size of the proofs and the computational effort required to verify them.

1. What is the usage of Difficulty Adjustment in Block Reward?

Bitcoin’s difficulty is designed to adjust every 2016 blocks — or approximately every two weeks. This adjustment is based on changes in the network’s hashrate, and occurs regularly in an attempt to ensure that the network continues to solve new blocks at a rate of one every 10 minutes. If the hashrate during the past two weeks has gone up, the difficulty will go up as well, making mining more challenging. If the hashrate has dropped, the difficulty level will decrease, making blocks easier to solve. The latter event is somewhat uncommon, and is considered by some to be a historically ominous indicator for Bitcoin’s price. When the next adjustment takes place, mining difficulty is expected to ease by 13.67%.

1. What’s the future of Libra in your perspectives?

I think it will be a global currency for billions of people, especially those in developing countries who have no access to banks or financial services. It will be the digital money which we can transfer to other people or simply use to buy stuff. I think Libra will not be a single currency that is backed by a basket of national currency but will now be a model of numerous individual fiat-pegged currencies.