Project Proposal: Data structures and algorithms needed for regulating Bitcoin

Member name: Xintang He, Kai Li, Zheng Liu

INTRODUCTION:

Bitcoin is a collection of concepts and technologies that form the basis of the digital currency ecosystem.[1] A unit of virtual currency called Bitcoin is used to store and transfer value between participants in the Bitcoin network. Bitcoin users communicate with each other primarily through the Internet using the Bitcoin protocol to perform currency functions, including buying and selling goods, sending money to individuals or organizations, or providing credit. Of course, Bitcoin can also be exchanged with other fiat currencies in some ways. Bitcoin doesn't have the concept of balance. It uses the model of UTXO (Unspent Transaction Outputs) to complete transaction. During the transaction, users have keys that prove that they own UTXO (balance) in the Bitcoin network.[1] Using these keys, they can sign transactions to unlock their UTXO and transfer them to the new owner address, then update the UTXO. After being public in Bitcoin network, the transaction is done. Bitcoin is a distributed peer-to-peer system without central control. Bitcoin was generated by solving complex mathematical problems, similar to mining. Any participant in the Bitcoin network can act as a miner, using its computer's processing power to verify and record transactions on the block and submit this block to the end of the block chain, thereby earning new Bitcoin rewards. In order to get the Bitcoin rewards, miners have to calculate a random value which meets a certain standard after twice hash operation(SHA256).[1]The miner who gets the right value first can get the rewards and his block would be added to the block chain. Libra is a currency released by Facebook and also a kind of cryptocurrency with block chain technology. Libra is a currency but not money, because Libra only serves as a medium of exchange.[2] Unlike decentralized cryptocurrencies (bitcoin and so on), Libra is not decentralized: 29 leading institutions from around the world form part of its consortium and this consortium is represented through Libra Association.[2] Meanwhile, Libra will function as stable coin tied to major government currencies to stabilize the value of Libra. Libra needs plenty of licenses to provide payment services in range of jurisdictions, such as a banking or other financial services provider license, licenses for its custody and safekeeping systems and so on.[2] However, Libra still have some risks such as operational risk, financial risk and systemic risk. Even though the real incentive for Bitcoin was to avoid regulatory agencies but we will address the question 'How bitcoin algorithms/data structures will change if it is regulated?". And in this short paper, we will propose a new data structure or an algorithm to make it possible to regulate Bitcoin.

Kai Li does the job that describing the knowledge of Bitcoin and the format check. Xintang He does the job that describing the knowledge of Libra and APA-style references. Zheng Liu does the job that summarizes this two knowledge and the spell check.

[1] Mastering bitcoin: Programming the Open Blockchain by Andreas Antonopolous

[2] Regulating Libra: The transformative potential of Facebook's cryptocurreny and possible regulatory responses by Dirk Zetzsche et al.