Project Proposal

Xiangyang Xu, Siyang Wu, Feng Liu

INTRODUCTION

Description of Bitcoin and Libra

Bitcoin is a collection of concepts and technologies that form the basis of a digital money ecosystem. Bitcoin users communicate with each other using the bitcoin protocol primarily via the internet, although other transport networks can also be used. In a sense, bitcoin is the perfect form of money for the internet because it is fast, secure, and borderless. Thus, Bitcoin is a distributed, peer-to-peer system and it is created through a process called "mining," which involves competing to find solutions to a mathematical problem while processing bitcoin transactions. Also, it has the protocol, which includes built-in algorithms that regulate the mining function across the network. Due to bitcoin's diminishing rate of issuance, over the long term, the bitcoin currency is deflationary. Furthermore, bitcoin cannot be inflated by "printing" new money above and beyond the expected issuance rate. Thus, bitcoin is also the name of the protocol, a peer-to-peer network, and a distributed computing innovation. (Mastering Bitcoin, Andreas Antonopolous, 2014, Chapter 1).

Recently, there comes another virtual currency which is Libra, it is the cryptocurrency project for which social media giant Facebook released the concept paper on 18 June 2019. To regulate Libra, Facebook lets Libra commit to open access to the blockchain, and open infrastructure, given that "open access ensures low barriers to entry and innovation and encourages healthy competition that benefits consumers.". Its value will be tied to a basket of major government-issued currencies and for each Libra issued an equal value of such currency, or highly liquid government bonds, will be placed on deposit with a reliable repository and it will also be a game changer. It signals the beginning of data giants entering in to finance in such a fundamental way as to have the potential, in poorer nations at least, to usurp many of the functions of the central bank, among others. (Regulating LIBRA: The Transformative Potential of Facebook's Cryptocurrency and Possible Regulatory Responses, Dirk A. Zetzsche, Ross P. Buckley, Douglas W. Arner, INTRODUCTION) In a degree, Bitcoin is similar with Libra which can be regulated. 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?". Thus, we will propose a new data structure or an algorithm to make it possible to regulate Bitcoin and below this paragraph is the possible ideal.

Prominent algorithms of Bitcoin -- SHA256 Algorithm (Secure Hash Algorithm 256)

"The algorithm for Proof-of-Work involves repeatedly hashing the header of the block and a random number with the SHA256 cryptographic algorithm until a solution matching a predetermined pattern emerges. The first miner to find such a solution wins the round of competition and publishes that block into the blockchain." (Mastering Bitcoin, Andreas Antonopolous, 2014, Chapter 2). Bitcoin uses SHA256 algorithm to determine which miner gets a bitcoin finally. SHA256 is a kind of algorithm that is easy to verify, but it's difficult to get the correct solution. It costs a lot of calculation power to get the correct solution.

INDIVIDUAL ROLE OF EACH TEAM MEMBER

Find and Analysis algorithms from paper: Siyang Wu, Xiangyang Xu
Implement algorithms: Siyang Wu, Xiangyang Xu, Feng Liu
Write Report: Feng Liu

REFERENCE

Andreas Antonopolous (2014). Mastering bitcoin: Programming the Open Blockchain

Zetzsche D.A, Buckley R.P, Arner D.W (2019). Regulating LIBRA: The Transformative Potential of Facebook's Cryptocurrency and Possible Regulatory Responses