# Assumption of Bitcoin Regulation Using Extra Basic Data Structures


1st Liu Feng
*ECE Department*
*Stevens Institute of Technology*
Hoboken, USA
fliu17@stevens.edu

1st Wu Siyang
*ECE Department*
*Stevens Institute of Technology*
Hoboken, USA
swu32@stevens.edu

1st Xu Xiangyang
*ECE Department*
*Stevens Institute of Technology*
Hoboken, USA
xxu46@stevens.edu



***Abstract*—Bitcoin is a decentralized digital currency without any banks or administrators. Since Bitcoin can be sent from user to user with no intermediaries, we decide to conceive a manner for regulating it. After the study about Libra (a cryptocurrency which is similar with Bitcoin), we use some basic data structures (Hash Table and Array List) as the assistance and apply the SHA256 algorithm in our work.**



***Index Terms*—Bitcoin, regulating, Libra, data structures, SHA256**


## I. Introduction

Bitcoin is a collection of concepts and technologies that form the basis of a digital money ecosystem. Bitcoin is created through a process called "mining," which involves competing to find solutions to a mathematical problem while processing bitcoin transactions and it also has the protocol, which includes built-in algorithms that regulate the mining function across the network. Due to bitcoin's diminishing rate of issuance, more and more company start to make their own cryptocurrency to take over Bitcoin's status. [1]

Recently, there comes another virtual currency which is Libra, it is the 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." [2]

In a degree, Bitcoin is similar with Libra. Even though the real incentive for Bitcoin was to avoid regulatory agencies, we still propose to use basic data structures and apply an algorithm to make it possible for regulation of Bitcoin.

## II. FUNCTION WITH DIAGRAMS

### A. Create a Server by Using a ArrayList (Siyang Wu)

Since the trade of Bitcoin needs no information of each user, it is very difficult for any institution to identify who made the deal. As far as we know, the blockchain of Bitcoin is consist of block nodes and the information inside each node is a string which containing cryptographic hash of the previous block, a timestamp, transaction data and a random number. And the Bitcoin user who can get the same result of the random number in the front block will get a reward and create a new block as the tail of the blockchain to record a current deal made by other Bitcoin users. However, this string is not enough for regulation and we need a server which can have a set of user's information (Miner, Giver and Payee). By using this server, we can track and search any validated Bitcoin users to prevent those illegal transfers from the transaction platform of Bitcoin.

If we want to regulate the Bitcoin, we must force every Bitcoin user to offer some solid information such as real name, phone number and local address in their own account. Based on this idea, we can use an Array List as the core of the server to store each user's account because the Array List has the high efficiency for searching every element inside itself. For example, if one of accounts of Bitcoin users is active, the server will match this account to every element of the Array List, if they match, this account can keep making the Bitcoin transfer or recording any Bitcoin deal made by others, if they can't, the server will reject any requests from this account.

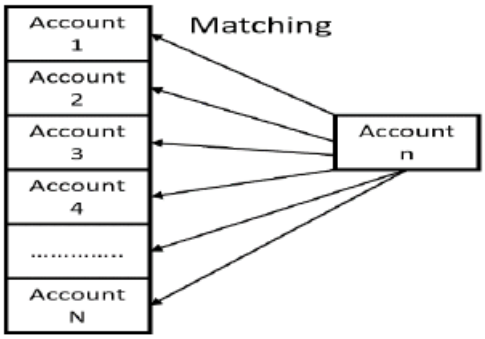


Fig. 1. Matcing in the Array List

## III. PSEUDO CODE

### A. Server's Part

## IV. CONCLUSION

Bitcoin is a decentralized cryptocurrency and has been criticized for its use in illegal transactions, its high electricity consumption, price volatility, and thefts from exchanges. Since the property of the blockchain of Bitcoin, it is very hard to modify any information of any transaction. However, if we

```
Algorithm – Matching
Input: Array List
Input: validated user account m
Input: user account n        # account needs to be identified
Index I = location of each account
Array. Length L = amount of the users
For I from 1 to L in Array List:   # store the user account
    Add user account m
For I from 1 to L in Array List:  # identify the user account
    if account n == Array[I]
      approved
    else
      rejected
```

use other extra basic data structures as a support to get an access to its blockchain just like what Facebook did to Libra, it will be regulated so how. In fact, it is impossible to fulfil the regulation of the Bitcoin and we hope our assumption can be applied to Bitcoin's system one day.

## V. CONTRIBUTION

In this work, Siyang Wu conceived the whole idea and composed the major part of this paper. Feng Liu has searched the algorithm for hash function and analyzed it. Xiangyang Xu has read the paper of the Libra and studied the property of the data structures we use.

## REFERENCES


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

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

[3] Cormen, Thomas H.; Leiserson, Charles E.; Rivest, Ronald L.; Stein, Clifford (2009). Introduction to Algorithms (3rd ed.). Massachusetts Institute of Technology. pp. 253–280. ISBN 978-0-262-03384-8.