

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. Strengthen Regulation of Bitcoin by implementing the HashTable (XiangYang Xu)

For the ease of getting the information of any users and the feedback of legality, we try to add a Hash Table to store every details of the Bitcoin trade. For example, if the server wants to know the validation of the user who is making the Bitcoin deal, his account ID (which is recorded in the Hash Table) will be sent back to the server. If this user is lack of their real name and other kinds of necessary information, his trade will be cancelled.

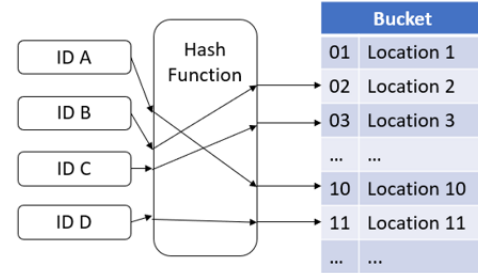


Fig. 1. Storing the trade information in a Hash Table

Hash Table is a basic data structure. The worst time complexity of Hash table is $O(n)$. [3] It uses a hash function to calculate the index into an array of buckets, from which you can find the required value. That means the object inside the Hash Table is a key-value pair. During the lookup, the key will be hashed and the resulting hash value will indicate the storage location of the corresponding value. According to this feature, we save the account ID as the key and the trading information of this user as the value into our Hash Table. For example, if we get the account ID, we can immediately require any details about each Bitcoin transfer.

As the Fig.4 shown, we add some extra information stored in the Hash Table into the block of Bitcoin's blockchain as the extra part of the string (original information in the block).

Take a block as the example, it contains two key-value pairs of our Hash Table. The key of the first pair is the current account ID who is sending the Bitcoin (giver ID) and the second one is the current account ID who will receive the transfer (payee ID). For the corresponding values of these two keys contain the same information which is other account IDs (former giver and payee) of previous block. If the value in the current block is identical to the current account IDs who made the Bitcoin deal in the previous block, the current block can be connected to the previous block otherwise the current Bitcoin transfer will be cancelled.

Beside the key-value part in the block, other parts of the information are miner's record (which Bitcoin user generated this block) and initial string which the original block giving to us.

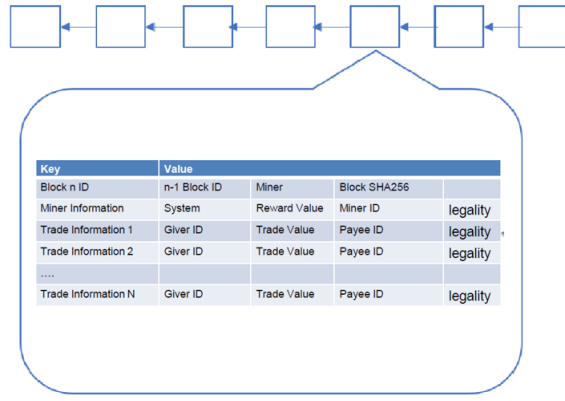


Fig. 2. Information inside the updated block of Bitcoin

In the Bitcoin trading system, miners are also the Bitcoin users. Thus, their legality also needs to be identified. Since the Array List to store every Bitcoin user's account, we can apply the same way of validating the giver and payee to a miner. For example, if a miner is recording a Bitcoin deal, the recording information and his account ID will be stored in the Hash Table as a temporary backup. Then we will send this ID to the server and if the server can't find the ID in the Array List, the miner will be identified as an illegal user and the record of the Bitcoin deal he is making will be committed to other legal miners who get the same random number as the string has.

III. PSEUDO CODE

A. Backup's part

The giver's ID and payee's ID will be the key to personal information. The server will verify the ID information after receiving ID and send the verification information to the Hash Table as the backup.

Algorithm – Storing	
Input: Hash Table Block	
Set K = key of Hash table	
Set S = storage location	
Set L = legality from server	
Set Hash() is the hash function	
For K in Block[key]:	
S = Hash(K);	# storage location
send S[0], S[1] to server;	# giver ID and payee ID
receive L from server;	# legality
S[3] = L	# add Legality to Value

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

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 Antonopoulos (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.