Regulating Bitcoin by adding license verification

1st Kai Li
kli41@stevens.edu

2nd Xintang He
xhe27@stevens.edu

3rd Zheng Liu
zliu110@stevens.edu

***Abstract*—Introducing a controlled model of cryptocurrency to show how can we regulate Bitcoin to prevent it from being used for illegal activities so that Bitcoin can better work as currency.In order to solve the problem of lack of regulation, we establish a central regulatory authority to manage the cryptocurrency.By doing so, only users and organizations who have license can issue cryptocurrency.To distinguish the normal account and special account, we use HashMap to encrypt the address.**

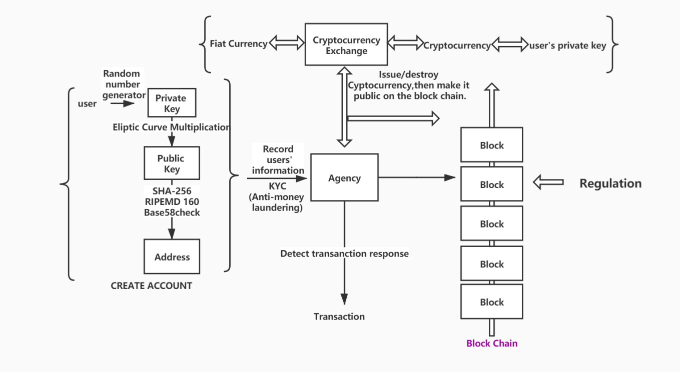
***Index Terms*—regulation, license verification, central agency, hashmap**

I. Introduction

Bitcoin is a collection of concepts and technologies that form the basis of the digital currency ecosystem. 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. 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 [1].

II. Cryptocurrency structure

We create an central agency to regulate the cryptocurrency and prevent it from being used for illegal activities. And it also can keep the stability of our cryptocurrency, make it possible to replace fiat currency.Agency has several functions.



cryptocurrency structure as shown above [2].

A. Create Account

Users submit a request. Agency will record users’ information to prevent anti-money laundering. Using random number generator to get the private key, then get public key by eliptic curve multiplication.Encrypt the public key by SHA-256 [3],RIPEMD 160 [4],Base58check, then we get the user’s address.

B. Cryptocurrency Exchange

Agency works as Cryptocurrency Exchange. It provides the service of exchanging currency. Users can exchange their Fiat Currency like US dollar, Euro, RMB to Crpytocurrency,vice versa.The exchange rate will strictly follow the basket of currencies to ensure the stability of cryptocurrency, strengthen its currency property and reduce speculation bubbles.

Agency also can issue or destroy cryptocurrency based on cryptocurrency exchange to stabilize cryptocurrency value. All the record of issuing and destriying crpytocurrency will be public on the block chain so that anyone can see it on the blockchain [5].

C. Publish Transaction

Aency will detect transaction response all the time. It will confirm transaction and get service charge. Then pack account book and make all transactions public on the block chain. All transaction can be traced by users’ address.

D. Regulation

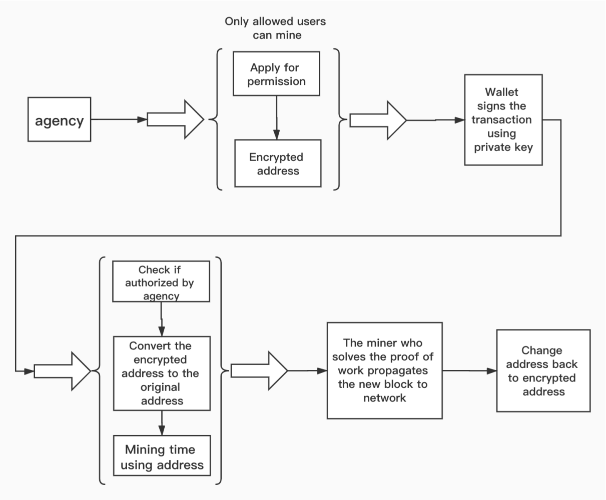
Account book, transaction, money chain are open to everyone and can not be deleted and modified.

Meanwhile, only the agency can match up the public key used for transaction with certain user. By doing so, we can effectively track illegal transactions and money laundering.

III. Agency Encryption Algorithm

This part is how the agency works and how it connected to Bitcoin. For the reason that currently, Bitcoin is not quite safe, we need to add some management system to make the transaction safer.

Names of the authors are listed alphabetically


Only allowed users can mine
agency
Apply for permission
Encrypted address
Wallet signs the transaction using private key
Check if authorized by agency
Convert the encrypted address to the original address
Mining time using address
The miner who solves the proof of work propagates the new block to network
Change address back to encrypted address

Use HashMap to store the information of original address, how many bits we added and what address we added. Then determine the user's legitimacy by determining whether the address is 36 bits and the address we get through HashMap is the same as original address.

A. *Encrypted Original Address*

Encrypt the original address through add the random(0,1) to its end, and then use a HashMap to memorize the address we add and the length of the address we add, then return the encrypted address.

B. *Decode Encrypted Address*

For the reason that we need to use original address to mine, so we need to get the original address. And we can get the original address because we store the information of the address we added by HashMap.

C. *Check If The Encrypted Address Is Valid*

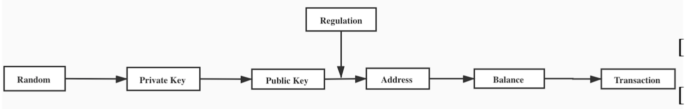
If and only if the address we can reach through encrypted address(target) is the same as original address, and the length of target is 36, then we can say this encrypted address is valid [6].

IV. Transaction

The transaction of Bitcoin is very complicated. There are many validation processes involved [7].

A. *Get Wallet*

First of all, there will be a random address, and this random address will be transformed to private key with some algorithm. Then we can get a public key from this private key. Wallet address comes from this public key. Wallet address will keep search all transaction in the block.



B. *Start Transaction*

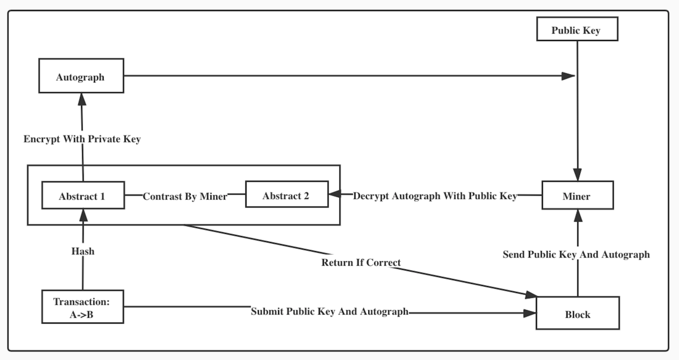
When someone make a transaction (For example A make a transaction to B), there will be generated an abstract-I by hash algorithm. Then the abstract-I will be encrypted with private key to an autograph. The autograph and public key will be sent to whole block. Block send public key and autograph to some miner.

C. *Validation*

The miner will get public key from A at the same time. Then the miner deciphers the autograph with this public key, and the result is abstract-II. Abstract-II will be contrasted with abstract-I. If these two abstracts are the same, the block will receive an order which said "hey, this transaction is Verified".

D. *Record*

Every transaction record like this processing will be kept in the block which will be checked in all the next deals. And miner can get their bonus when they deal with these validation process. One transaction can only be admitted in the block when all transactions before it is approved.



So, in my opinion, if we want to make the system of Bitcoin run under regulation like Libra but keep its non-centralization. The best way is to find an algorithm that can transform the public key of those who voluntarily accept regulation to a new one. In order to get the new under-regulation key, you have to submit an application attached with your personal information to the agency and wait for approval and your new key. Those who get a new under-regulation key can do everything with their bitcoin and others may get some restriction.

Acknowledgment

Thanks Professor Aftab Ahmad for your guidance during the project. It helps us find the direction and overcome a lot of problems.

References

[1] A. M. Antonopoulos, *Mastering bitcoin: Programming the open blockchain*. " O'Reilly Media, Inc.", 2017.
[2] D. A. Zetzsche, R. P. Buckley, and D. W. Arner, "Regulating libra: the transformative potential of facebook's cryptocurrency and possible regulatory responses," *University of New South Wales Law Research Series UNSWLRS*, vol. 47, 2019.

[3] H. Gilbert and H. Handschuh, “Security analysis of sha-256 and sisters,” in *International workshop on selected areas in cryptography*. Springer, 2003, pp. 175–193.

[4] H. Dobbertin, A. Bosselaers, and B. Preneel, “Ripemd-160: A strengthened version of ripemd,” in *International Workshop on Fast Software Encryption*. Springer, 1996, pp. 71–82.

[5] R. Böhme, N. Christin, B. Edelman, and T. Moore, “Bitcoin: Economics, technology, and governance,” *Journal of economic Perspectives*, vol. 29, no. 2, pp. 213–38, 2015.

[6] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to algorithms*. MIT press, 2009.

[7] M. Moser, “Anonymity of bitcoin transactions,” 2013.