Digital currency rating

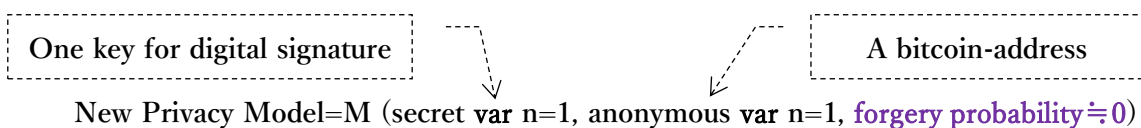The multivariable n (n $\geqq$ 2) blockchain is the prototype of "money": represented by the function M ().

"money"=M (secret var n=1, anonymous var n=1, multi-variables n=3, forgery probability)

Here, the multivariable IDs n=3 of M () represents three digital $ID_1 \neq ID_2 \neq ID_3$, and n represents the number of random variables: secret variable≡a private key, anonymous variable ≡a bitcoin-address.

This prototype is the mother body of Bitcoin, stable coin, peg currency, CBDC, multivariable digital currency, etc. The mother's body knows various "money" ratings. Let's count the number of prototype variables: 1 + 1 + 3 = 5, ➡ Rating = 5. The smaller the number of variables, the lower the rating. Conversely, the system becomes more stable as the number of variables increases. It's easy to imagine that two variables will be more stable and controllable than one.

1) Satoshi Nakamoto's New Privacy Model

> One key for digital signature   A bitcoin-address
>
> New Privacy Model=M (secret var n=1, anonymous var n=1, forgery probability≒0)

The New Privacy Model is the prototype of Bitcoin. Here the number of variables is 2 in total, so Rating = 2. However, in actual operation, a password is allowed to access the secret variable. So the variable is not a random variable, but just visible data (anyone can see it when they have the password). Therefore, the New Privacy Model is destroyed as follows:

"money"=M (secret var n=1➡n=0, anonymous var n=1➡n=0, forgery probability≒0)

> If the variable turns into visible data, it becomes the target of cyberattacks and internal crimes.

Since 0 + 0 = 0 here, Rating = 0. The computational relationship is a secret variable ➡ a public variable ➡ an anonymous variable. If the secret variable changes to "visible data", the currency forgery probability is likely to be 1, but Bitcoin is not. Since it is mining, the probability of counterfeiting≒0. Although it deviates from the main subject here, the mining cannot meet the demand for money.

2) mere IT_ "money-like" of surveillance society_

To the eyes of the CCP authorities, both anonymous and secret variables are just "visible data."

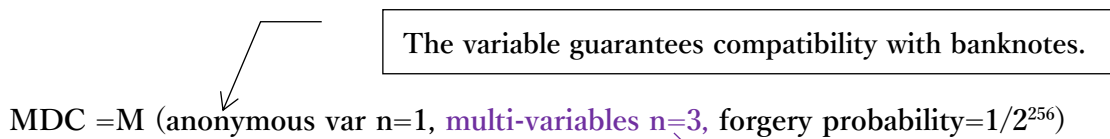People are assigned a unique ID, and the ID is linked to "visible data."

Digital RMB=M (secret var n=0, anonymous var n=0, forgery probability=1)
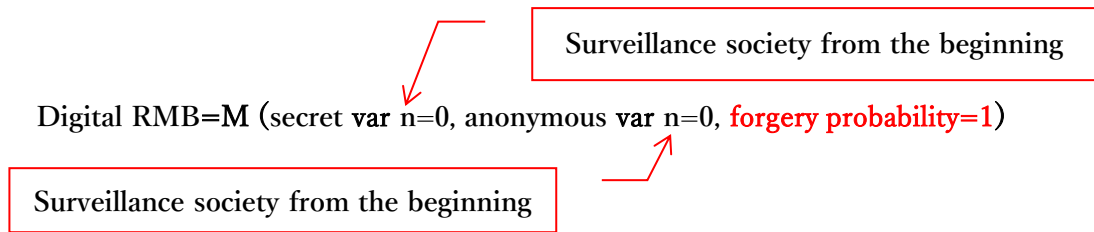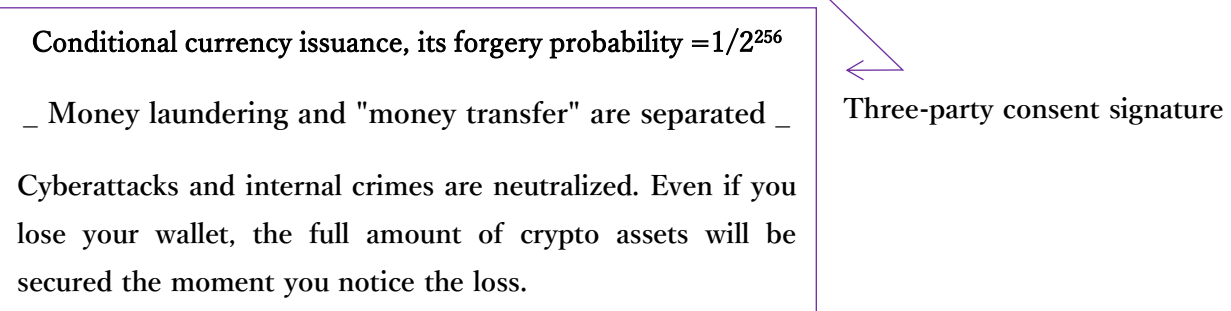
Here 0 + 0 = 0, so Rating = 0.

The above formula is based on the assumption that the digital yuan is designed on the basis of blockchain. The digital yuan does not mine, that is, it meets the demand for money: what does this mean? Counterfeit probability = 1. The digital yuan has been "issuing counterfeit currency" from the beginning. There is a way to hide counterfeiting: splitting the network into wholesale and retail sales. In any case, the world is deceived.

3) Multivariable digital currency (MDC)

The following explanation of M () is given in the main text.

The variable guarantees compatibility with banknotes.

MDC =M (anonymous var n=1, multi-variables n=3, forgery probability=$1/2^{256}$)

Here, 1 + 1 + 3 = 5, so Rating = 5.

Conditional currency issuance, its forgery probability =$1/2^{256}$

_ Money laundering and "money transfer" are separated _

Cyberattacks and internal crimes are neutralized. Even if you lose your wallet, the full amount of crypto assets will be secured the moment you notice the loss.

Three-party consent signature

September 28, 2020
©Author
Eiji Watanabe
METEORA SYSTEM