Subject: Multivariable Digital Currencies

Subtitle: This article is the story of "Inventions that prevent digital currencies from becoming money laundering and terrorist financing."

Dear friend:

Before reading the main text, I will explain the main points of the invention without explanation. The blockchain itself is a historic invention, but everyone hasn't mastered it yet. Initially, stakeholders had high expectations, but they were not able to use the blockchain as expected. Price volatility and money laundering are only valued negatively. I see its price volatility and money laundering as an important potential "wild horse" and buy it high: because I know how to train it.

Trainer's eyes

Why does fiat money just printed on paper pass from person to person? If you think about it like this, you can see why: If a person sees fiat money and then sees your privacy, it would not circulate. The same is true for gold and silver. This thought experiment shows that the New Privacy Model designed by Satoshi Nakamoto (Paper) is important: this is the starting point for "money." I would like to ask the reader the following questions to confirm this starting point: *When paying at the cash register, do you type your password on the banknotes?*

The above question reminds us of the difference between mere IT and "money": anyone interested in this difference must be an ambitious entrepreneur or pioneer. I, the trainer, also see this difference. Banknotes do not require a password. Similarly, multivariable digital currencies do not require passwords. *Are you relieved if you are asked for a password?* Even if you have a password, if the cyberattack succeeds, your crypto assets will disappear. And insiders can reach the password.

Digital currency at the moment is "mere IT" that destroys New Privacy Model

I hear that in 2020, central banks in each country will form several groups to work on digital currencies. I can imagine the digital yuan: CCP has already established a legal system to collect information on cashless payments at the People's Bank of China (1). Since it is the currency of the surveillance society, Satoshi Nakamoto's New Privacy Model is ignored from the beginning. Personal ID and payment flow in a surveillance society are linked: no privacy. If the authorities stop using the ID there, whatever the transfer of money will stop. This is a "mere IT" story, not a currency story. It is unclear whether the digital yuan is designed based on the blockchain, as it is legally promoting a surveillance society. In any case, the world is being fooled by the

digital yuan. ☞ digital currency rating

Similarly, I think the authorities of democracies will have a discussion close to the digital yuan. Rather than discussing the design of "money," authorities will also discuss the design of "mere IT": that is, they will ignore the importance of the New Privacy Model. For example, it does not aim for a surveillance society, but requires the submission of personal information (KYC). That is mere IT, IT that sacrifices privacy. Japan has various social infrastructures such as resident's card, health insurance card, driver's license, etc., so there is no shortage of IDs. However, it is "My Number" with one more ID. Because of this tendency, there is a possibility of introducing My Number even in the case of digital currencies: This will make Japan the same as the CCP surveillance society.

Digital currency rating

I have a mirror here, "Function of money≡M()". I decided to show the multivariable digital currency, Bitcoin, and mere IT in this mirror. ☞ digital currency rating. Please check which function has the lowest rating here.

Inventor's eyes

I have experienced that the world does not choose the best: what people are looking for is not the best. Schumpeter says, "You only think about connecting one carriage to another. Connecting them doesn't make a train ...". It is very difficult to abandon the carriage-to-carriage connection thinking. So I look forward to ambitious pioneers and entrepreneurs: I would like to tell them not only the deterrent of crime, but also how to train rampage horses, below.

Social implementation of blockchain

Money laundering and money transfer are separated: Cyberattacks are also neutralized.

In multivariable digital currencies, the key for signing (a private key) is "burned" and there is no key data: the key exists only as a function. The ash that remains after burning is called the multivariable digital IDs n = 3: the expression n = 3 means three variables. Cryptographically speaking, this situation of "burned and no key data" means that the key data for signature has become a pre-image of multivariable digital IDs n = 3. The key data is an image!

Each of the three variables is implemented in the blockchain society (user, Xchange, third party): no key is implemented. In each case, the will of society is divided into either agreement or disagreement as to whether or not to extend the signature chain. This alternative is a new innovation that makes it possible to control digital currencies and/or blockchain. It leads that:

1) If any Bitcoin address is suspected of money laundering, disagreement of the society occurs, and Xchange will intervene and stop the procedure. At the same time, make a "public call" and see the response to separate the true and false of the flow.
2) Since there is no key data in the blockchain society, there is no target for cyberattacks. This perfectly protects the consumer's crypto-assets. In addition,
3) when a consumer loses his wallet, he will get all the crypto assets back in his possession, as long as he notices the loss.

Conditional issuance of digital currency

4) The social implementation of the three variables established the "subject responsible for the issuance of money".

That Bitcoin mining is not a mechanism to meet the demand for money. I saw "the subject responsible for issuing money" in the n = 3 social implementation. Digital currency is, of course, a signature chain defined by Satoshi Nakamoto. Stealing the key data for this signature allows for a large amount of forgery: no one notices the key leak because it's not a scene where a terrorist fires a machine gun and steals it.

There are two names for this subject: one is A) a monetary base with three variables, and the other is B) a social implementation with n = 3 variables. A) pays attention to the difficulty of currency forgery. B) pays attention to price control. Both respond immediately to the demand for money. This makes it possible to control price volatility. In other words, it is possible to draw a gentle ascent curve like the S & P 500 without killing the potential of the rampage horse.

Availability

When I started writing this document, on May 1st, I was in the corona pandemic. There were many worries ... Not only in Japan, but also in the coronavirus or catastrophes, there is a strong force that incites fear, people are inflamed by fear, and people destroy the economic base for people. … Democracy falls into the trap of big government, and people go to the trap on their own. Central banks and supply chains are exhausted, and of course, small and medium-sized enterprises are also exhausted ... The attraction of the trap is getting stronger and stronger. But now my worries are gone. Even if the facts of the future turn out to be worrisome, it's time for a currency that the private sector can launch, I have: the availability of multivariable digital currencies.

This paper focuses on two points: "deterrence against crime" and "conditional issuance of digital currency". Therefore, it positions the third party as an institution that monitors money laundering and terrorist funds. When considering the availability, think of the third party as a

position to restart society, restart the economy, and restart politics in pursuit of happiness. What this means is that it is a currency issued by the private sector, "a self-sustaining currency." It may be said that it is not money for economics, but a currency aimed at giving joy to people's self-help efforts. Neither Marx nor Keynes knows such a currency. As a reference for knowing the position of the third party, Swift coin is included in the appendix of the main text. With the above, I would appreciate it if you could participate in the discussion of multivariable digital currencies.

From here to the text PDF

Best regards

Eiji Watanabe

METEORA SYSTEM

September 20, 2020

Body table of contents

[Technical data link list]

Satoshi Nakamoto (Paper)

Blueprint for multivariable blockchain

digital currency rating

Implementation example of multivariable n = 2

(1) Magazine “The Liberty” December 2019 No. 298

Print this Hyper text