Multivariable digital currencies

This article is the story of "an invention that prevents digital currencies from becoming money laundering and terrorist financing."

In honor of the pioneer Satoshi Nakamoto....

Think deeply about bank accounts and banknotes. According to Japanese customs, a "conditional withdrawal" is performed with two IDs, a passbook and password, or a bank card and password. Here the two IDs are random variables: we will denote them by ID_1 and ID_2. It is difficult to determine ID_2.from ID_1, and vice versa. So the two variables are independent. We know "conditional withdrawals": if you enter ID_1 and ID_2 *"in line"* at an ATM, the banknote will come out. The important thing is to "enter the two together".

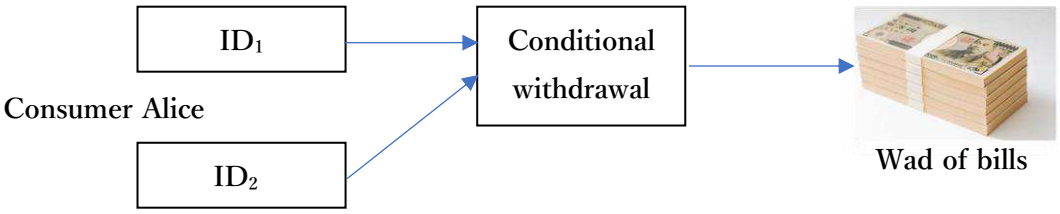


Fig.1: Multivariable IDs n=2

If two events happen to meet accidentally, it becomes a "complex problem" of conditional probability: However, ID_1 and ID_2 here are promised to be "two in one". Such a promise (protocol) is called multivariable IDs n = 2.

The incident happens when the ID is stolen: it also happens when it gets lost. So if Alice withdraws a lot of money, the bank may ask for a "confirmation of Alice's identity". This is the third ID ≡ ID_3. Now control the withdrawal by aligning the three. This is the multivariable IDs n = 3.

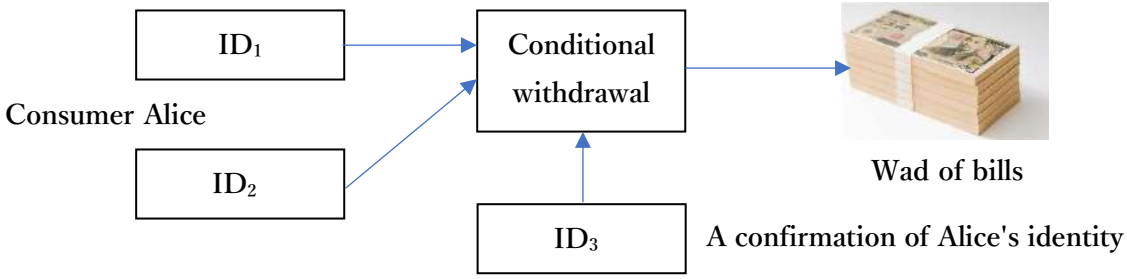


Fig.2: Multivariable IDs n=3 that aligns three IDs

Here, let's confirm the definition of electronic coins designed by Satoshi Nakamoto (☞ This link is on the Hypertext screen): “We define an electronic coin as a chain of digital signatures.” (Cited

from 2 Transactions). Let's project this definition on Fig. 2: The light of the signature chain shines on the "wad of bills". Then "conditional withdrawal" would be "conditional signing procedure". The projection is as follows:

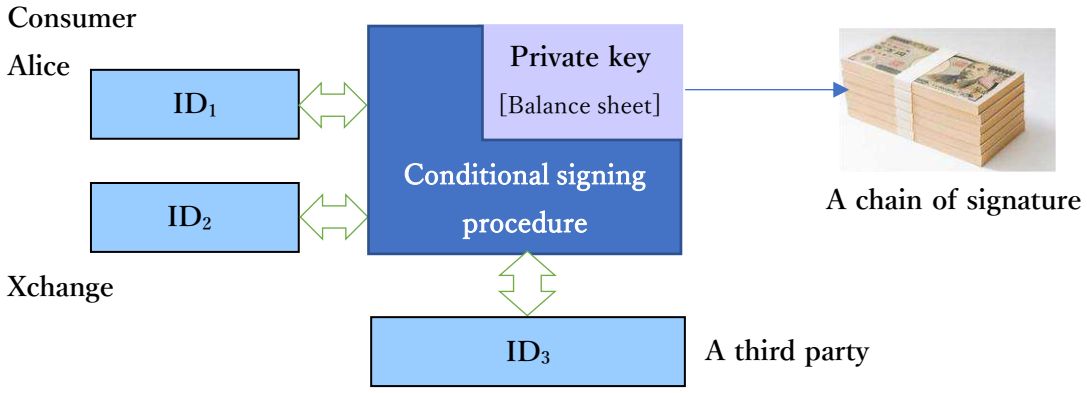


Fig.3: Conditional signature procedure

The signing process begins when all three IDs are complete: Conversely, if the IDs are not complete, nothing starts. Such a conditional signing procedure is not described in Satoshi Nakamoto's paper.

New definition of digital currency

There is no protocol that conditions "transfer of money" in the design of Satoshi Nakamoto (☞ This link is on the Hypertext screen). Introduce a new definition of digital currency: Conditionally execute the following signatures:

Withdrawal = Remittance = Currency issuance

What are the conditions? As Fig. 3 shows, 1) ID_1, ID_2 and ID_3 are each owned by Consumer, Xchange, and a third party respectively: 2) Three parties (Consumer, Xchange, a third party) agrees to sign the above process. There is cryptographic mathematics to verify this consent:

Collision function that verifies the consent of the three parties

The verification of consent of the three parties is divided into "no objection" / "with objection". "There is an objection" is when any one of the multivariable IDs n = 3 is missing, or when any two are missing. In this case, the key data for signing is not reproduced (the signing procedure is interrupted). This interruption is fail-safe. Continue the following status:

Freeze remittance = Freeze money laundering assets = Stop issuing currency

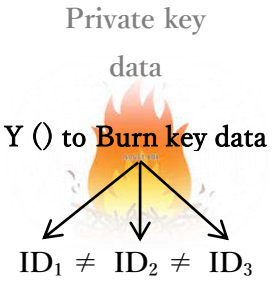
Note that privacy is protected here and no one's "face" can be seen. This is an important criterion for distinguishing between "money" design and "mere IT". Since "mere IT" requires the registration of personal information, the authorities can see the "face" of the user. The above is the prologue.

Ⅰ. Key management innovations

Multivariable digital currencies have a number of innovations: 1) The signing key exists as a function, but is not implemented: 2) Cyberattacks are neutralized: 3) Money laundering and normal money transfer are separated: 4) Instead of mining, there are digital currency issuers: 5) It is difficult to forge digital currency(Attacks on the issuer of currency from inside and outside is not successful). Since there is only one technology base that supports these innovations, I will introduce it.

1. Function to burn a private key_ remaining ashes_ multivariable digital IDs n = 3

Needless to say, the private key is a key for signing. Satoshi Nakamoto defined Bitcoin as a signature chain (cited from 2 Transactions). The theme I am presenting now is not Bitcoin, but multivariable digital currencies. Multivariable digital currencies are also signature chains like Bitcoin, but they are signature chains based on the "conditional signature procedure" shown in the prologue. This technology base is unique. First, the function Y () that burns Private key data, what remains after burning is "ashes", and this concept is illustrated below.



Y (), which burns Key data.

After inputting the key data in the function Y (), delete the key data.

Multivariable digital IDs (ID_1, ID_2 and ID_3) appear in the output of the function Y ().

The remaining ashes are multivariable digital IDs (ID_1, ID_2 and ID_3). Ash has the following relationship: $ID_1 \neq ID_2 \neq ID_3$. This inequality means that it is difficult to calculate and determine each other. There is also a vertical calculation as opposed to this horizontal calculation. That is, even if I calculate the private key data from $ID_1 \neq ID_2 \neq ID_3$, the answer "This is it" is not returned.

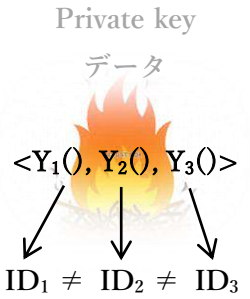
The above function Y () is expressed in a unique form: $Y() \equiv <Y_1(), Y_2(), Y_3()>$

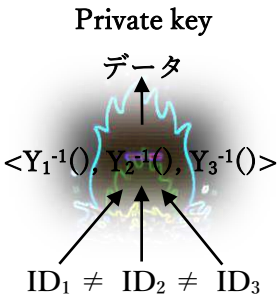
2. Collision function

There is an inverse function of the function Y (): it is the "collision function $Y^{-1}()$". The function $Y^{-1}()$ restores the key data from the ashes. It is expressed as: $Y^{-1}() \equiv <Y_1^{-1}(), Y_2^{-1}(), Y_3^{-1}()>$

The illustration below shows the function that burns Private key data on the left and the

function that restores key data from ashes on the right. The two functions relate to my patent.



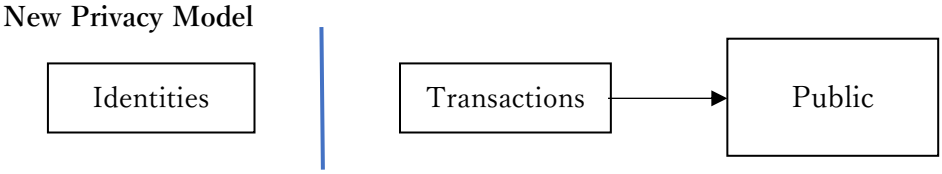


Add these functions to Satoshi Nakamoto's paper, which is Blueprint for the multivariable blockchain: (☞ This link is on the Hypertext screen)

Ⅱ. Compatibility with fiat money

1. Satoshi Nakamoto's New Privacy Model

Originally, the blockchain was designed so that there was no central authority. So money laundering is possible. In this case, money laundering can be tracked but the "face" is not visible One thing to note here is that money laundering can be tracked. ➡ It is possible to track the transfer records of money, but the "face" is not visible. Satoshi Nakamoto (paper) named this mechanism the New Privacy Model. Let's look at the illustration he drew.



The blue line in the above figure shows that the privacy drawn on the left side is protected and all transactions on the right side are open to the Internet. Then, "Privacy is not interfered by the government (power organization), but the remittance record is made public." Isn't fiat money the same?

New Privacy Model is compatible with fiat money

Now, assuming a "digital currency?" that ignores the New Privacy Model, you'll find that it's just "IT," not compatible with banknotes.

IT that requires the registration of personal information and passwords, this is not "money".

A "digital currency" that acts as "money" in a surveillance society or a country is able to deceive the people with "mere IT." *However,* the currencies handled by Xchange move freely across borders. What happens if other currencies compete with "multivariable digital currencies" here?

There is a case like this: Let's say you went to cover a new kind of "xxx coin" as a magazine reporter. You asked the following question in the middle of the explanation: "What if the smartphone is stolen?" ... "No, don't worry, look, you're safe because you have a password, right?" the answer came back. You asked more questions: "That means the authorities know the flow of money. It's also convenient for tax collection, right?". I would like to ask another question: "Can passwords prevent cyberattacks?"

2. Current because it protects privacy:

At the beginning, "Dear Friend," I asked, "Why is fiat money just printed on paper current?" The answer lies in the "New Privacy Model": "Fiat money is current because it protects privacy." Bitcoin shares the same formula:

Bitcoin = New Privacy Model

So why did Bitcoin become a financial product and not a currency? There are two reasons. One is that it does not have a mechanism to meet the demand for money. The other is below.

3. Anonymous variable and private variable

The New Privacy Model can be likened to an armored car: anyone can see the cargo, but not who goes to whom. About this car Satoshi Nakamoto (paper) [10 Privacy] says: “The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone.”. Further on: “privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous.”.

Explain: The public key here doesn't have an X.509 certificate, ➡ I don't know who the public key is, ➡ So I don't know who the Bitcoin address is, so it's an anonymous variable. There is another one, secret variable: Private key. Since the number of variables is one each, it is expressed as n = 1. Project these facts into the "money function M ()":

M (anonymous variable n=1, secret variable n=1) = New Privacy Model

This is a formula that privacy is protected *if the secret variable is not leaked.*

Initial public offering of Bitcoin company!

Service designers, *however,* design to register passwords somewhere. When a password works with an anonymous or private variable, the variable becomes "visible."

Bitcoin ≠ New Privacy Model

This makes Bitcoin incompatible with banknotes. This incompatible Bitcoin is an initial public offering of Bitcoin Co., Ltd., and is by no means a currency. In fact, Bitcoin today is found in the portfolio.

Ⅲ. Cryptocurrency freezing protocol against money laundering

1. Restrict the use of Bitcoin addresses _does not sacrifice privacy_

When the digital yuan makes a remittance, it is a conditional remittance: If the authorities like Alice, make a money transfer: If the authorities do not like Alice, limit Alice's freedom and stop the remittance: That is, the digital yuan(RMB) limits Alice's freedom. On the other hand, multivariable digital currencies restrict the use of Bitcoin addresses rather than specific person Alice. So don't sacrifice privacy. A conditional signature is required for this.

The New Privacy Model does not show a "face", but provides a mechanism to verify the flow of remittances from the past to the present: Verify the ownership chain. However, until now, there was no way to control this remittance flow even if it was known to be fraudulent. In other words, we can see the fraudulent money transfer chain, but until now there was no way to control it. But this time it's different:

Collision function to verify the consent of the three

Now suppose the reader wants to break the fraudulent money transfer chain at this moment. However, at this stage, it is still undecided whether it is fraudulent or not. That wish is easily fulfilled: Restricting the use of Bitcoin addresses in fraudulent chains: That's all.

Therefore, one of the multivariable IDs combined with the Bitcoin address is moved off from online operation. In this way, the system interrupts the signing process. The protocol says: One of the IDs n = 3 does not collect at the entrance to the "collision function" so the key data for signature cannot be reproduced: ➡ Remittance is interrupted:

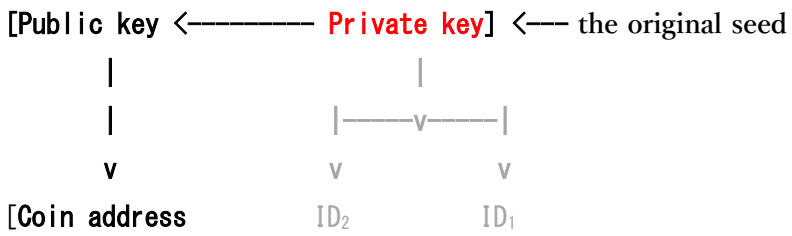
Suspension of remittance = Suspension of money laundering assets

The issue now emerges: how to associate the Bitcoin address with the multivariable IDs.

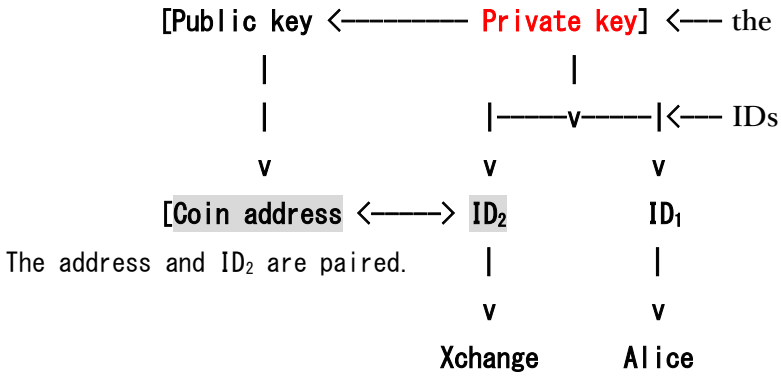
2. Link the Bitcoin address with the ID_2 of the Xchange:

Normally, Alice keeps ID_1 at hand, transfers the second ID_2 to the Xchange, and transfers the third ID_3 to a third party. This is the "social implementation of multivariable IDs n = 3".

Combining a Bitcoin address with one of the multivariable digital IDs is easy: it can be done at the hands of Alice. This is because both Bitcoin addresses and multivariable digital IDs are based on Private key data. Since Alice is the only person who has the original material, Alice can link the two: a third party cannot. The process is:



The direction of the arrows is easy to calculate: right-to-left arrows are used for signatures: top-to-bottom arrows are used for verification of an ownership chain. Here, the number of multivariable IDs is set to n = 2: The bitcoin address is written as Coin address.



Make a pair of ID_2 and Coin address at Alice's hand. Deliver this pair to the Xchange: The Xchange stores this pair in the DB. Here the Xchange does not know who the pair is: Alice's privacy is thus maintained.

3. Money laundering freeze protocol.

Introducing a protocol that uses ID_2,(one of the multivariable digital IDs) as a control variable: The protocol moves ID_2 off from online operation. This alone interrupts the remittance.

Now suppose a report comes to the Xchange that the Bitcoin address (Bob) and the Bitcoin address (Oscar) may be dark side addresses: The judge is usually a third party with ID_3. This third party usually monitors money laundering. Alternatively, the Xchange may have determined that the remittance flow is suspicious.

Conditional signatures, Public call and Failsafe, this set is a money laundering solution

When such a report came, the Xchange stopped the online operation of ID_2 and made the following public announcement on the net ... We stopped the operation of the coin address (Bob) and the coin address (Oscar). If you have any objections to this, please contact me ...The second variable ID_2 will not return online without any contact in response to the call. ➡ Money

laundering assets are automatically frozen (Fail-safe based on the nature of the blockchain).

The freeze protocol above is fail-safe based on the nature of the blockchain. If the intention of money laundering responds to the "public call", the "face" of that intention will be revealed: If there is no response, the "remittance procedure interruption" cannot be canceled. ➡ It can be said that it is an automatic asset freeze. This protocol can be applied not only to money laundering, but also to insider trading, market manipulation, and court asset conservation orders.

Basis for financial sanctions

The legality of the surveillance society is the basis for the financial sanctions imposed by the digital yuan. My invention is not based on centralized power, but on the basis of public calls and fail-safes for financial sanctions.

IV. CBDC matter, Conditional issuance of digital currencies, Fair price control

Conditional currency issuance _Solution different from mining_

1. Are you relieved if you have a password?

Banknotes are real: the process of picking, touching, and handing is real. No one wants to register a password on banknotes. In comparison, cryptocurrencies are more airy: I don't have "this" to say "this is mine". Can you protest when one day you are told, "It's an incident, your crypto assets have disappeared!" So when you are asked to register a password, do you feel relieved? But if anyone wants to steal, the password can be stolen.

Multivariable digital currencies do not require password registration. There is no object that you want to protect with a password. The private key is required for signing, but its key data is not implemented. Therefore, there is no reason to ask for password or biometric registration. "It's an incident, your crypto assets have disappeared!", This can only be joked.

One day, Alice realizes she doesn't have a wallet: she may have misplaced it somewhere, or she may have dropped it. When you drop your wallet, the bills usually don't come back. You might think that multivariable digital currencies have the same fate as banknotes because the multivariable does not have any password. That's right, it's the same as banknotes.

I think multivariable digital currencies should have the same fate as banknotes, but Alice wants to protect all of her crypto assets. How about the following wristbands for such people?

Alice realizes that she does not have a smartphone and immediately notifies the Xchange (or a third party) with the second variable ID_2. This variable ID_2 has a CIM parameter, ➡ The Xchange turns off the operation of variable ID_2 from online ➡ The remittance procedure is interrupted. The problem here is to notify the exchange (or a third party) immediately. how? Since the backup device stores the multivariable digital IDs, urgent messages fly from here to the Xchange via the nearest base: the message has variable ID_2 and a CIM parameter. Imagine a backup device: a wristband comes out.

For wealthy Alice

"Wristband" and smartphone make up Alice's wallet. The device has only a transmission function. The Xchange has a procedure to cancel the remittance interruption.

2. Privacy-to-privacy transfer chain

Multivariable Digital Currency (MDC), Bitcoin, Digital RMB were projected onto the money function M () and rated: ☞ Digital currency rating (☞ This link is on the Hypertext screen). The functional form of multivariable digital currency is as follows:

MDC = M (anonymous variable n=1, multivariable IDs n=3, forgery probability=$1/2^{256}$)

There is an anonymous variable n = 1 here: there is no secret variable n = 1. Therefore, no Key data is leaked: Multivariable digital currencies chain from privacy to privacy. This is different from IT, which sacrifices privacy. It is also different from "xx coins" and digital yuan, which sacrifice privacy for convenience. The figure below shows time progressing from left to right:

Privacy	Forming a chain,	Privacy
Backup of IDs		Backup of IDs

Fig.4: Privacy-to-privacy transfer chain

How to form a chain is described in Satoshi Nakamoto (paper) [3. Timestamp Server].

3. Three party-consent verification, "trust of money" instead of mining

Overview

Normally, when consumer Alice registers with a Xchange, Alice has ID_1, while transferring the second ID_2 to the Xchange and the third ID_3 to a third party: the Xchange or the third party identifies smartphones with CIM parameters: Each of the three is independent of each other. This is the "social implementation of the number of variables n=3". Two fruits can be harvested from this social implementation: 1) crime deterrence (brake role) and 2) money trust (accelerator role).

1) No remittances will be made without the consent of the three parties: this will fail-safe against accidents and crimes. This is the braking role.
2) Having a collision function that verifies the consent of the three parties is more reliable than a settlement made by a single will. This is the accelerator role.

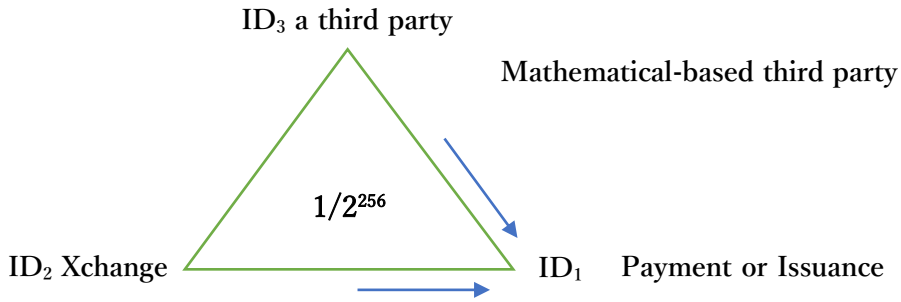


Fig.5: Three-party consent verification = Digital currency issuer

Figure 5 shows a diagram of the consent verification of the three parties. Applying this to CBDC, the issuance of digital currencies naturally should be based on the will of the central bank, but the behavior of IT at the time of issuance is not a single-will protocol. Originally, there is no issuer in blockchain mining. The mechanism for verifying the consent of the three parties is the issuer of digital currency.

Mathematical-based third party

The third party in Fig.5, even if it simply receives a third ID_3 and monitors fraudulent remittances, can make a significant contribution to the reliability of payments. Mathematical science is more reliable than a centralized payment and remittance system that costs a lot of money. There is a case where this mathematically based third party makes a great contribution: One of the embodiments is "Swift coin". Appendix (☞ This link is on the Hypertext screen).

Three-party consent verification chain

In Fig.5, the social implementation of the number of variables n=3 is represented by a triangle, and the arrows represent how the variables ID_1, ID_2, and ID_3 are gathered in the "collision function". Key data for signature is reproduced in the output of "collision function" ➡ The

currency issuer updates the signature chain (remittance).

Satoshi Nakamoto defined Bitcoin as a chain of digital signatures. "We define an electronic coin as a chain of digital signatures." (Cited from 2 Transactions). Following this, multivariable digital currencies are also defined as " Three-party consent verification chain". An illustration of this definition is Fig. 6: Time advances from left to right.

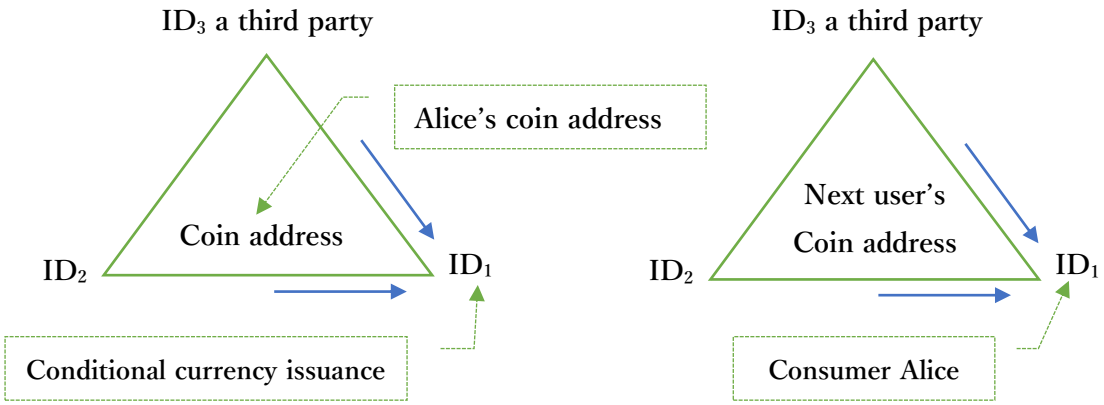


Fig.6: Three-party consent verification chain

Description of the figure:
Conditional currency issuance sends money to Alice's Bitcoin address: (left ➡ right): Alice sends money to the next user's Bitcoin address. If the currency issuer is a central bank, it may transfer an electronic coin to consumer Alice via a Xchange (private bank) or a third party. In any case, Alice validates the ownership chain and sends money to the next user's Bitcoin address. This is a chain of conditional currency issuance.

Anyone would instinctively believe that a three-party consent verification chain is more reliable than a single-will signature chain. Let's calculate how reliable it is. I will calculate the difficulty of creating a fake coin. Before that, there is something the reader wants to know.

How would the current blockchain issue the CBDC?

1) Mining cannot meet the demand for money. There is no entity responsible for issuing currency. If you forcibly put it on the market, as you know, it becomes a financial product.

2) Assuming that the central bank and government bonds have credit, if a remittance of 1 million yen is recorded on the blockchain, does it mean that 1 million yen has been issued? That is not the case. Because the key data that signed 1 million yen may be the leaked key data: No one notices the leak of the key data. Authorities must have a history of distribution to distinguish between counterfeit money and legitimate money: This is a surveillance society. My

patent is the only way to stop the leak of the secret variable n = 1. ☞ Section I

3) In the olden days, authorities tried to meet demand by mixing gold with copper. Assuming that the mining solution is solved by the same method, passwords and biometric information are combined with anonymous variables and secret variables in operation. If so, would you want to have a "xx coin" at the expense of privacy? I'm sure you will go to a Xchange office. If you meet with a multivariable digital currency app, you can sell "xx coins" without hesitation.

Difficulty of making fake coins, overwhelming reliability and stability

The world still doesn't know a clear solution to the problem of key management. Let's look at digital currency ratings again: ☞Digital currency rating (This link is on the Hypertext screen)

MDC = M (anonymous variable n=1, multivariable IDs n=3, forgery probability=$1/2^{256}$)

Since IDs n=3 is the "ash" that remains after burning the Private key data, no Key data is leaked from the function M (). The reader cannot make a counterfeit money.

So ... let me create a counterfeit money for multivariable digital currencies. Counterfeit money is to steal Alice's key data, make coins, and send them to someone's Bitcoin address. The collision function was introduced on page 3: where when multivariable digital $ID_1 \neq ID_2 \neq ID_3$ is input to the collision function, a collision occurs and the key data is reproduced in the output. An attacker with this knowledge draws the following scenario: Hijacking any one of the communication paths of $ID_1 \neq ID_2 \neq ID_3$, throwing an arbitrary random number to cause a collision, and stealing the output data from the inside or outside:

How many attacks will cause a collision? Of the 2^{256} times, one collision occurs and the key data is reproduced. This is a brute force attack. The probability of a collision = $1/2^{256}$. In fact, can 2^{256} attacks be allowed on the net? I think it's very difficult to make a counterfeit money.

Timestamp required for payments made by a single will

The current signature chain is updated with a single will, so a time stamp is needed. ☞ Satoshi Nakamoto [3. Timestamp Server]. The current bank online system also completes payment with a time stamp.

On the other hand, the three-party consent verification chain is irreversible in itself: the following reasoning. As mentioned above, the probability of making counterfeit money for multivariable digital currencies is = $1/2^{256}$. There is no distinction between this counterfeit money and regular coins. The probability that the next user will succeed in making a counterfeit

money from the counterfeit money is = $(1/2^{256}) * (1/2^{256})$. This chain is a time stamp: the same reasoning as Satoshi Nakamoto's [3. Timestamp Server]. Therefore, it turns out that it is more reliable than the settlement made by a single will.

4. If you have a multivariable digital currency, you will get a bonus!

This is a bonus article: The content of the article gives the private sector a lever to launch a multivariable digital currency. Useful in the future.

We have identified multivariable digital currencies as "Three-party consent verification chain". This entity is not the single will of the currency issuer, but a system consisting of the currency issuer, the Xchange and a third party. Key data for signing is not implemented here, but the currency issuer can perform digital signatures. The following effects can be expected.

Now suppose Alice sent money from her bank account to my account: it charges a fee. I will bear the fee; then I will get a negative bonus.

If Alice sends money in multivariable digital currencies, it comes with a positive bonus for me. The reason is as follows: When Alice sends me money, Alice buys multivariable digital currencies on the Xchange; the seller is an unspecified person, including the issuer of that currency. The three-party consent verification chain is responsible for maintaining a fair price.

The currency issuer adjusts the fair price according to the rules and sells. When I receive the multivariable digital currency, I can exchange it for banknotes, or keep it as it is, my freedom, my privacy. This currency guarantees my privacy by mathematics, not by the legal system: probability theory guarantees my freedom.

If I don't exchange, I'll keep my multivariable digital currency, just like the banknotes I keep at home: because multivariable digital currencies are compatible with banknotes. I'm willing to sell if it's above the price I received: this is a bonus. Since there is an issuer (three-party consent verification), it is possible to control price declines and surges: It allows a gradual price increase such as S & P500.

Appendix (☞ This link is on the Hypertext screen)

Swift coin, super-profitable interbank remittance, future image of key currency

Summary

Issuance of fiat money is a credit item (liability) of a central bank. The mechanism is a single will of the central bank. Blockchain mining is not a single will and cannot meet the demand for money. So the CBDC has no choice but to abandon mining and become a "domestic digital currency" operating in a closed network: assigns a unique ID to consumers and requires password registration during retail payments: As a result, like the digital yuan (RMB), it becomes a "money-like" of a fine surveillance society. The rating calculation is 0 + 0 = 0 ➡ "Rating=0". ☞ Digital currency rating (This link is on the Hypertext screen). "Rating=0" has a fatal weakness: There is no reason for people to buy the "money-like" of the surveillance society. However, it exerts a mysterious power in a democratic society.

The People's Bank of China "sees" all cashless payments under the law [1]. There is no such legal system in Japan, but when the "Rating=0" CBDC is implemented in society, it will become a surveillance society and will be finished as a "big government" against the background of tax collection power. It is magic that the Chinese Communist Party's surveillance society will be realized in this way in a democratic country. I don't want to see such a "carriage-carriage connection show". I want to see a train. The train is the issuance of a digital currency with a "rating = 5".

I pay tribute to Satoshi Nakamoto: he defined electronic coins as a chain of digital signatures, yet made all participants anonymous variables. Following his insight, I was able to define a "three-party consent verification chain": No password registration is required. It treats consumers as anonymous variables from start to finish, protects privacy, separates money laundering and normal remittances, operates on the Internet. No key data is implemented in this program. Therefore, this is the definitive methodology for making blockchain quantum resistant: it is also an implementation means.

At the end

I am 80 years old now. I don't know when it will end. It may be in the countdown. I want to disclose the whole invention within five years, for posterity. I estimated the duration of the disclosure work to be 5 years: I decided to ask someone to buy my disclosure work. I can't bring money to "heaven", so I entrust contracts and votive money (license fees) to investment in posterity. That is, set up a foundation to invest in your countries.

The disclosure work will help drive your business. It includes "license agreement" and

"copyright sharing". In addition, the agreement also includes the idea of how to handle the gain on issuance of currency (seigniorage).

The license you obtain is a "promise to limit my rights". So I will accelerate your business. It will be disadvantageous for those who come later, but it is natural that the person who dug the well first is given priority. I look forward to your feedback from blockchain stakeholders, enterprises, central banks. Questions are also welcome.

October 07, 2020

© Author
Eiji Watanabe
METEORA SYSTEM
eiji-dualcontrol@ozzio.jp
patento-info@meteora.co.jp

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