March 22nd, 2020

White Paper of Crypto Cash

Research Institute of Information Security
Representative Director Takatoshi Nakamura

＜Background＞

As mankind began to feel barred in bartering, money was devised as a means of indirectly exchanging value, and cash transactions were born. Compared to the credit economy that is based on the credit of the traders, the use of cash with an entity issued by a trusted issuer does not necessarily require the credit of the traders. Because trading can be done with big amount and frequency, cash transaction is considered an indispensable form of transaction in modern economics.

In modern times, there are three basic functions of money: "payment means", "value storage means", and "value scale". Money was made from specially shaped stones or rare shells in ancient times and evolved to be made by metals and paper as its media, but what was developed from the mid-20th century to end the problem of counterfeiting and fraudulent use is the ultimate currency, "Crypto Cash".

The first Crypto Cash, born around 80's, was a fixed-price type that stores encrypted data in information storage areas on a plastic card, and was called plastic money. Suica, which is widely used in Japan, is considered to be the successor to these plastic moneys, but the current value rechargeable system allows counterfeiting and fraudulent use and fails to realize the original purpose of Crypto Cash.

Later, in 1983, Dr. David Chaum of the United States showed that encrypted currency information alone is enough to create Crypto Cash, and it was commercialized as DigiCash in 1989. The idea that making Crypto Cash using only encrypted currency information means that "digital cash" can be created, and a number of companies followed after DigiCash.

Around 1995, when Windows 95 was released and the Internet browser Netscape is introduced, the Internet was about to transform from a mere bulletin board for professionals into a main battlefield for commercial commerce, and Crypto Cash gained attention as an essential tool for this commerce, it were as if the Cambrian era of new Crypto Cashes. New Crypto Cash concepts were announced one after another, put to practical use, mainly in the United States and the United Kingdom. Thinking about it now, there was no way to make truly secure Crypto Cash because of the incomplete and incomplete cryptography of the time.

Completion of cryptography itself was indispensable for the completion of Crypto Cash, and it took another ten years.

Two years after the world's first true Crypto Cash was completed, one attempt was made to put it into practice under the name SATOSHI NAKAMOTO. It was Bitcoin. If you try historical examination, it is probably a paper at the same time as DigiCash, a trial draft of a non-cash-based "ledger" method before DigiCash, using imperfect cryptography at the time. Use a hash chain that has been

used for more than half a century as a ledger. Although there is nothing new technically to be seen as a whole, there is a feature in that by having all participants have the same ledger, falsification of the ledger is prevented by a majority decision method using a huge cost. It takes a certain amount of time to reach a consensus, during which all members confirm that there is no doubt in the details of the transaction (authenticity check), and confirm that they have not been used before (double use check). Whether it was fortunate to be seen democratic because it was a majority decision method, or just for speculation purposes, it gained some enthusiastic users. However, 51% attacks on Ethereum, a leading cryptocurrency (virtual currency), and Bitcoin, earlier this year, is about to end blockchain systems.

＜Crypto Cash＞

"Crypto Cash", the world 's first cryptic cash, is an entity currency that uses a string of symbols encrypted using perfect cryptography as an indirect substitute for value exchange. Issuer information and value information of cash are uniquely associated with completely encrypted symbol strings, preventing counterfeiting and fraudulent use. By encrypting conditions such as credit information, usage conditions, interests, deadlines, Crypto Cash having various functions can be created. Since it does not depend on media, metal cash can be created by carving Crypto Cash on it or banknote can be created by printing Crypto Cash on paper. As with conventional currency, since it has entity of symbol string, it has three basic functions of "settlement of value", and "storage of value", "scale of value".

As well as currency based on metal or paper cash, Crypto Cash can be issued as a legal tender based on national governmental credit or as a convertible ticket with another legal currency. But like Hong Kong's legal notes, it can be issued by issuers such as banks or global companies. As guarantee of trust, it is also considered to be issued using the value of natural resources, in addition to precious metals such as gold and silver as collateral.

In the first place, cash is indirect substitute for value exchange, between two people, the smallest unit of value exchange, the value (or credit) that each other trusts is exchanged by exchanging its direct substitute which corresponds uniquely one by one. In the case of Crypto Cash, this is just an encrypted symbol string and it is nothing different from conventional cash. It prevents from counterfeit or fake use, and thus it is a better substitute with an unprecedented feature of not choosing a medium.

For this reason, most of the current currencies are issued based on the decision of quantities and schedule in advance, and generally the government or central bank distributes currency to the market by storing and managing it.

After confirming the issuer and the value, Crypto Cash encrypts it using complete encryption technology and issues encrypted cash information (symbol string). When using Crypto Cash, be sure to confirm authenticity and unused, and then the recipient holds or receives it. Higher safety can be ensured by updating to new encrypted cash information (symbol string) each time.

In summary, Crypto Cash is composed of the following four core functions and is used in combination with the application system according to the purposes.

a. Credit (collateral) check function
   Confirm the conversion with legal tender or collateral. Add to the cash information the banknote number in the case of legal currency, and the mining information in the case of natural resource collateral which are reserved and numbered.
b. Crypto Cash issue function
   Crypto Cash is issued by completely encrypting issuer information and value information.
c. Crypto Cash storage and management function
   Store and manage already issued Crypto Cash, and adjust the market distribution volume.
d. Crypto Cash authenticity check function
   When using Crypto Cash, check whether it is genuine or not yet used. Incidentally, the confirmation information can be recorded openly using a crypto ledger.

Crypto Cash was originally developed to prevent counterfeiting and fraudulent use of fiat currencies, but applications are being prepared; such as relief of conventional crypto assets that are collapsing, issuance and management of crypto securities / bonds, and issuance and management of crypto insurance.

<Example>

＜Example of Crypto Cash＞

In addition to “server issuing type” Crypto Cash, ″user issuing type″ Crypto Cash can also be realized and it is issued every time the user of Crypto Cash uses it. In other words, it is possible to build a system that allows not only centralized authorities but also any individual to issue Crypto Cash. In such cases, as with the conventional personal check, it is issued as collateral by personal deposit, prepaid remaining amount or credit balance. In addition, you can use it like traditional debit cards, prepaid cards, credit cards, etc. without worrying about theft or fake use, which is said to exceed $ 1 trillion in the world. The installation is easy because no dedicated card reader or dedicated line is required.

As a practical example of Crypto Cash, the debit card type Crypto Cash (DC-CC) which can prevent the card fraud which has increased rapidly in recent years (for example, illegally acquiring card number and improper use) is explained here.

In order to use the DC-CC, the user opened an ordinary account at the bank, then install a DC-CC dedicated application on his/her smartphone and activate with a pass code secretly given from the bank for the preparation. Then, DC - CC is used with the following procedure.

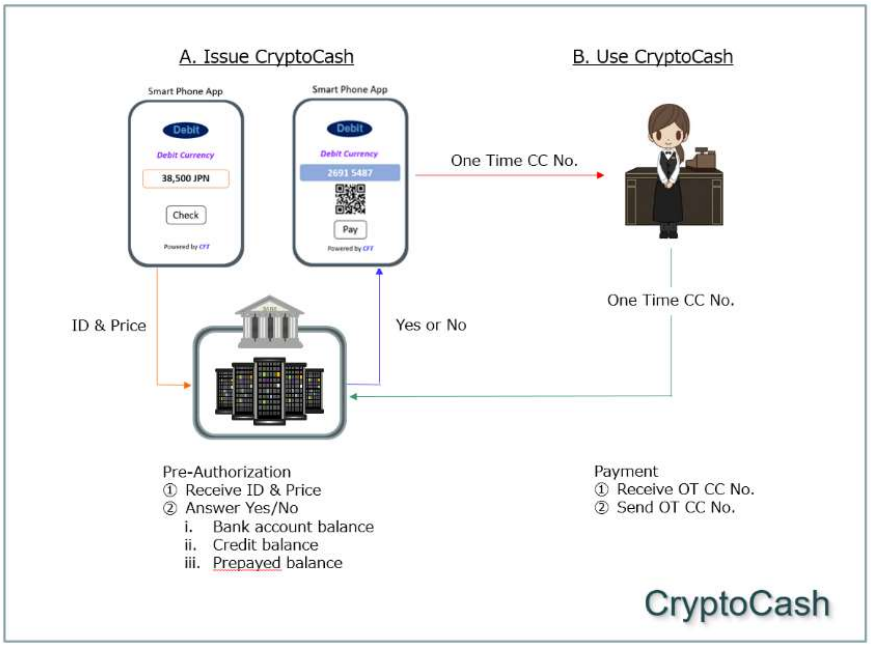
① Start the smartphone debit card type Crypto Cash application, enter the settled amount of

38,500 yen (example) to the window of the phone, for example, then the application sends it to the bank server together with the user ID.

② If the balance is sufficient, the bank server gives issuance permission to the application of the smartphone, the application on the smartphone issues an 8-digit debit cash number which is effective only for 5 minutes, possible to settle the exact amount of 38,500 yen, and is used only once. This debit number is obtained by encrypting information specifying a value of 38,500 yen, for example.

③ Tell the shop this number and the shop will send this number to the bank server.

④ If the settlement is successfully completed, a signal of termination of settlement is sent to both the user and the shop and the process is terminated, but if it fails, reissue the debit cash number and start over.

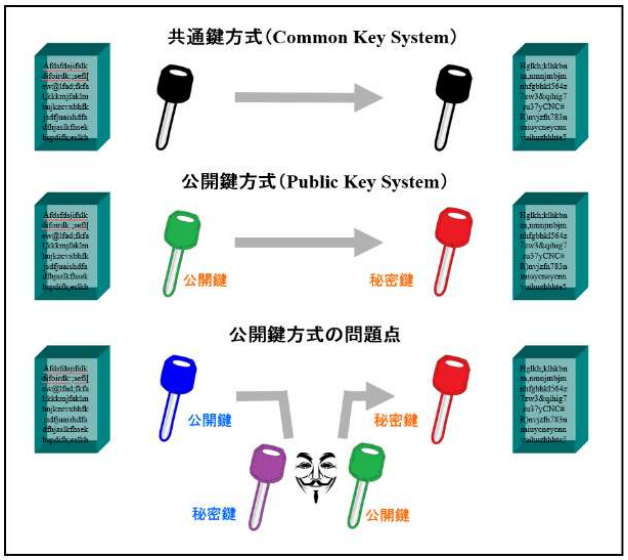


Reference 1: Public key system and its defects

Public key system is currently the most widely used cryptosystem, centered on Internet security. In order to overcome the "problem of encryption key delivery" which is the biggest problem of the common key system which has to share the encryption key beforehand between the encryptor and the decryptor, in the 1970's, James Henry Ellis (1924 - 1997) and Clifford Christopher Cocks (1950 -) and Malcolm John Williamson (1950 -) in UK and Bailey Whitfield Diffie (1944 -) and Martin Edward Hellman (1945 -) in USA found the public key system, an

encryption key to be encrypted and an decryption key to be decrypted are configured by pairs different from each other.

A ciphertext encrypted with a public key can be decrypted only by a paired secret key. If such a pair of keys exists, if all the information sent to the party is encrypted with the public key, only the person with the private key can decrypt it. Even if a hacker gets a public key, it cannot decrypt it. As a result, the public key can be opened to anyone to use it, so it came to be called public key system (PKS).



Generally, it has been said that it is practically impossible for computing power and time to derive a secret key from a public key, and therefore cannot be deciphered in practice. In RSA cryptography mathematical problems called "prime factorization problem" is used and in elliptic curve cryptography "elliptic curve discrete logarithm problem" is used. However, since a long encryption key is used for public key system as compared with the common key system, the calculation time is enormously required, and it is often used only to deliver the encryption key of the common key system, and now it is supposed to be believed to solve "encryption key delivery problem". Since public key can be published beforehand in the public key system, it is optimal for the Internet era, and widely used such as electronic bidding, SSL, blockchain and so on. As the computing power improves, the possibility of deciphering increases, so that attempts have been made to lengthen the key length in order to overcome the vulnerability each time. However, as we enter the quantum computer era, we cannot solve it by merely lengthening the key length, as mentioned above. NIST in the USA and others began to work on a new standard quantum-resistant encryption algorithm that can be used after the quantum computer era and they call for new algorithms. However, as a further fundamental problem, the problem that the authenticity of the public key is not easily certified was revealed. Currently, the public key certificate issued by trusted third parties (Trusted Third Party, TTP) is widely used and this method is called public key infrastructure (PKI). However, no matter how many certificates are attached, even if a root certificate is used as a certificate of certificates, it is clear that counterfeiting cannot be prevented. That is even the initially expected "encryption key delivery problem" has proved to be never resolved.

Reference 2: Complete encryption technology

Cryptographic technology consists of encryption algorithms and encryption keys since ancient times. In order to strengthen the encryption, it is conceivable to ① make the encryption algorithm more complicated or ② increase the number encryption keys. However, even if the method ① or ② is extremely good, it is impossible to create a cipher that cannot be deciphered. Most of the current cryptographic technologies are based on what a huge amount of computation is necessary to decipher and it is the fact that it cannot be said that it is never decipherable. Therefore, when the performance of the computer improves, the possibility of being deciphered increases, so it is necessary to use a more complicated encryption algorithm or to increase the number of encryption keys by lengthening the encryption key length. In the quantum computing era of the near future, cryptographic technologies which are theoretically undecipherable are required.

The answer to this challenging problem in this human history is the encryption scheme devised in 1918 by Gilbert Sandford Vernam (1890 - 1960) who worked for AT&T, and in 1949 Claude Elwood Shannon (1916-2001) proved undecipherable under certain conditions and this algorithm is called Vernam cipher or one-time pad.

It is impossible to decipher when the cryptographic key shared between the encryptor and the decryptor in advance is truly random and the length of the key has the same length as or longer than the plain text to be transmitted. However, it has been said that sharing an encryption key of such a length is not practical so far. This is because if the encryption key of the same length as the plain text can be shared, it is enough to share the plaintext itself.

As described above, the final tasks for developing the ultimate cryptographic technology are two, which are "indecipherable algorithm problem" and "problem of encryption key delivery" at present. If "problem of encryption key delivery" is resolved, cryptographic technologies that solve "indecipherable algorithm problem" such as Vernam cipher can be used and completely confidential communication becomes possible.

The "public key system" was said to solve this "encryption key delivery problem", but after that, a fatal defect was found. Furthermore, although the ultimate solution has been said quantum key distribution (QKD) using quantum cryptography, even using quantum cryptography, it is not always possible to communicate with an authentic opponent. If the eavesdropper succeeds in pretending as the correct recipient, it can communicate directly with the sender using quantum cryptography, obtain all the information, and resend the correct information or false information to the correct recipient.

Currently, there exists a complete encryption technology that has been proved to solve both of two problems, "indecipherable algorithm problem" and "encryption key delivery problem", which is called “Complete Cipher” and it is used for Crypto Cash.