

CIPHER CORE



Provide a next generation evolutionary cash platform that can issue
crypto token/coin which is regarded as the
historical final form

~ Truly democratic freedom of crypto token/coin issuance
to all individuals/communities ~

(Project Overview)

Currently, it is reported that the on-line theft exceeds 1 trillion dollars in the world, but fundamental solution has not been provided yet.

Ever since the Internet was opened to private sectors in the 1990s, commercial transactions on the Internet have grown explosively and have changed the traditional business custom fundamentally. And the world has dreamed of creating cash that can be used safely on the Internet. Proposals for more than a hundred new cash originated at the dawn period disappeared due to the vulnerability and no alternative was shown until crypto cash, the true crypto currency, appeared.

In the meantime, the necessity for cash that can be used on the Internet has been increasing, and experimental attempts to use the ledger in 2009 have been shown to the world. This is Bitcoin using a blockchain. Although Bitcoin demonstrated new ideas such as double trading prevention and consensus building of all participants in the community, it has already begun to cause many problems due to structural vulnerability and limitations.

Meanwhile, the momentum for communities worldwide to issue tokens/coins (private coins) unique to the community different from legal tenders issued by the government is increasing ever, and already 1,600 tokens/coins have been issued worldwide using blockchain technology or its applied technology and a new economic sphere appears. It is not stoppable to issue tokens/coins even though conventional blockchains which are the basic technology for issuing tokens/coins are breaking now.

Therefore, we decided to provide a crypto cash platform by applying crypto cash technology which was designed originally for issuing legal tenders. This means that all issued (and will be issued) tokens/coins will be able to be evolved to crypto cash which will be the final form of historical currency by shifting to this new platform. Anybody in any community can issue any crypto cash that can be used on the Internet that does not require huge amounts of communication traffic or electricity, can be instantly settled and can be saved.

And, CIPHER CORE evolves to the first crypto cash on the Cipher Core Platform.

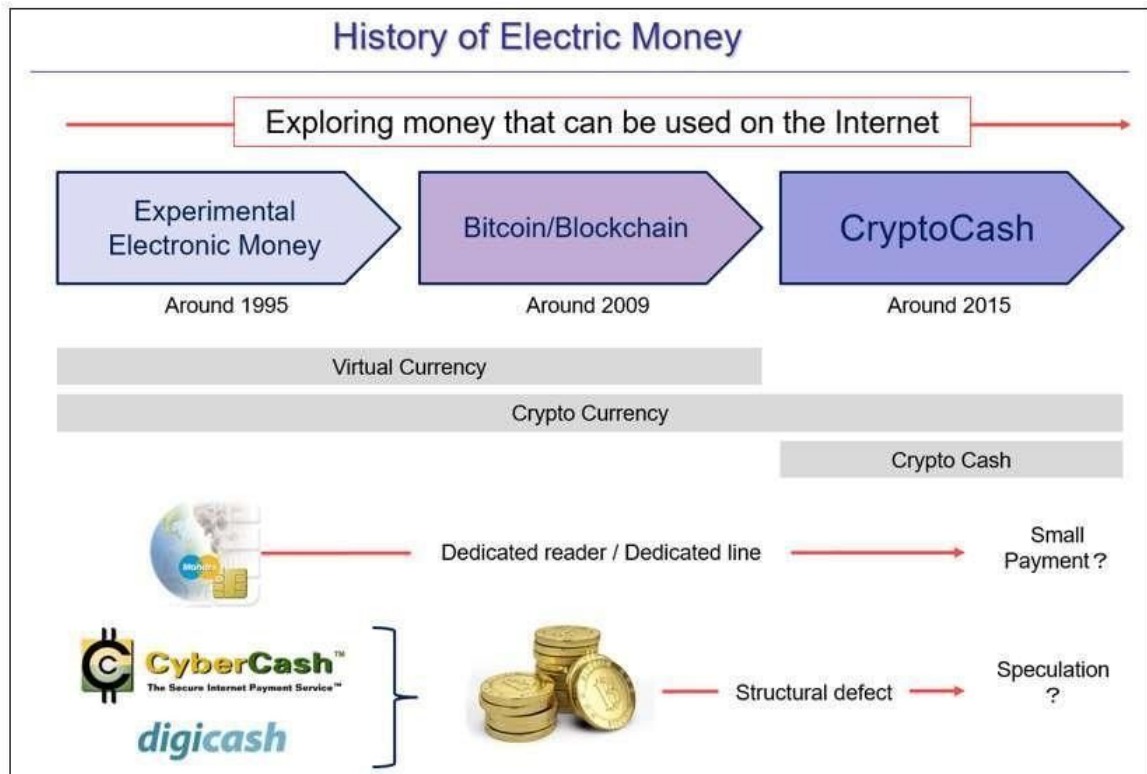
(Project Background)

Since ancient times, mankind has developed a huge economy beyond the tribe, beyond the continent by inventing currency having three functions "means of settlement", "means of storing value" and "value scale". Currencies are issued using beautiful seashells, gigantic stones, or precious metals. In modern times national governments issued banknotes that are convenient for carrying with credit of the state as the basis. While adverse effects of counterfeit currencies are widely perceived, crypto cash, which is unforgeable, thus said to be its final form, started to appear finally.

The Internet invented in the 1960s became commercially available in the 1990s, and in 1993 the World Wide Web (WWW) and the first browser Mosaic were released. In the following 1995, when MS-DOS most widely used is upgraded to Windows 95, many pioneers who anticipated explosive increase in commercial transactions on the Internet tried to start inventing crypto currencies (data as a pseudo tangible article with value). By 1995 more than 100 new ideas were introduced and commercialized. However, there were no projects that could have reached the new century. The cryptographic technology was not mature enough to create cash to be used on the Internet yet. Human beings had to wait for the completion of cryptographic technology for the appearance of true crypto cash.

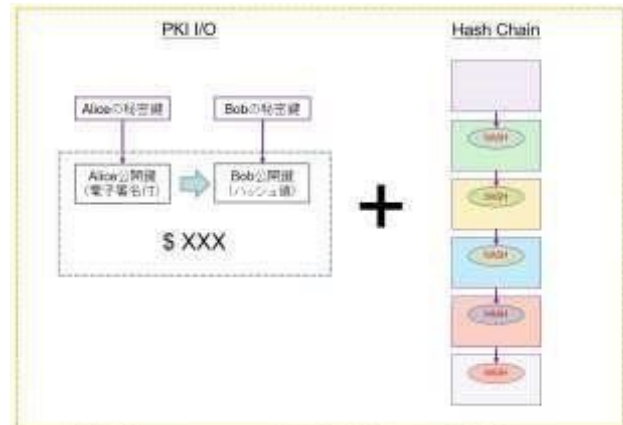
In the last year of the 20th century, a new standard of cryptographic technology which already reached a level where vulnerability cannot be overlooked was decided, but still it did not reach the level at which crypto cash could be created. However, in 2009, for a completely different purpose than the contribution to humanity, the pre-modern experimental attempt was introduced that used the technology of the 1990s, thus encompassing great vulnerability. The first purpose which is creation of cash used on the Internet was abandoned, and easy method was used which researchers of the 1990s with high pride never used. This is a Bitcoin using a blockchain and is generally considered to be a variant of the cryptographic currency, not crypto cash. Conventional currency completes settlement at the same time as that exchange. There is no need to record a ledger every time. On the other hand, the value of Bitcoin depends on the accuracy of the ledger. Therefore, it is only important how to accurately record and keep this ledger accurate, so immediate settlement is sacrificed, and even old settlements may be overturned in order to maintain accurate ledger. It was a great achievement to make crypto currencies known to the whole world even with such incomplete system, however, less than one month after the lecture of the collapse of the

blockchain in San Francisco in August 2017, China government made a Bitcoin prohibited, the magnificent experiment came to an end.



(What is a blockchain ?)

A blockchain consists of a data storage part that uses a hash chain and an input / output part that uses PKS (public key system). A hash chain is an old technology that creates a database that cannot be altered from the middle or from the opposite by calculating a hash value of a chunk of a certain data and making it a part of the next chunk of data and repeating this to create a continuous data chunk string.



In addition to the above basic structure, the blockchain is the addition of the following functions.

- 1 Always update a large number of identical copies of the hash chain so as not to overturn past transactions.
- 2 In order to prevent double transactions, only one person at a time adds transaction information.
- 3 Rewarding system to run.

Incidentally, the hash function used here is a function that converts the data into a fixed length numerical value when certain data is given and has the following features.

- 1 All sizes of files are converted to fixed length values.
- 2 The same hash value is always obtained from the same data, and the hash value obtained from even different data at all becomes completely different.
- 3 The conversion is one way, it is impossible to derive the original data from the hash value.

For example, in the electronic signature, a hash function is used for reduction of the capacity of the signature target and detection of tampering in the hash function, and in the TCP as the standard protocol of the Internet, it is used for checksum for confirming the lack of communication data.

(Collapse of blockchain supporting virtual currency)

A blockchain has attracted attention as a non-tamperable entry system that functions even without a central administrator. Sometimes it is described as a distributed ledger, but the reality is that it is not a distributed ledger consisting of a single ledger, but it is a large number of identical copy ledgers with exactly same contents. In order to make it impossible to tamper with it, it is necessary to prevent falsification of the ledger itself. Although tampering is almost impossible as a blockchain uses hash chains for data storage, it is inadequate. If the whole ledger is replaced, falsification will succeed.

Thus, a blockchain makes it impossible to tamper the entire ledger by duplicating many copies of the same contents. Even so, problems such as rewinding of the blockchain that makes the transaction canceled after a certain point of time, attack taking advantage of the long length of time to add a next block and, etc. are reported. Why it became necessary to have a large number of copies in the first place originally is that one transaction becomes effective after it is recorded, and then its current situation is proved only by checking all the past transactions. It is the largest defect of the ledger system.

As a result, internal problems such as the following are reported for this blockchain at present.

- 1 Ledgers (blockchains) exceeding 100 gigabytes have appeared, and there is a possibility that it will be forced to be corrected because of the ever-increasing transaction volume of the ledger near future.
- 2 Sharing of a huge ledger (blockchain) has the possibility of "data missing" in the file sharing P2P method, so now full replication is required to share.
- 3 As a result, enormous amount of communication and electricity are required for duplication of the same ledger, and maintenance of a large number of copies is becoming difficult.
- 4 Sustainability of blockchain systems is becoming suspicious since compensation corresponding to mining is becoming not enough, and companies that stop mining are emerging. There actually started to appear coin platforms in which the blockchains are effectively stopped.
- 5 Even the daily transaction book keeping alone requires a huge amount of electricity and communication volume.

Meanwhile, there are three cases (external attacks) caused by the public key system (PKS) which is responsible for reading and writing to the blockchain, as the followings;

- 1 Lost or stolen private key from wallet or deposit.

- 2 Although PKS is not necessarily only reason, a blockchain has weak point which is managed only with a private key, and many incidents exploiting the private key have occurred.
- 3 Transaction contents are tampered by man-in-the-middle attack (MITMA). For falsification of transaction contents by MITMA, the following attacks are reported.
 - a) The login information is stolen by an attacker impersonating the exchange.
 - b) Transaction contents are tampered with the systems such as Myetherwallet before using the blockchain API. Although it is not exactly classified as a man-in-the-middle attack, the possibility of receiving the following attacks is pointed out by malware entering Wallet.
 - c) Make money illegal transfer from wallet of full blockchain at hand (access to blockchain P2P directly).

Moreover, major problems related to operation have been pointed out.

- 1 Due to disagreement, fork happens easily. If countermeasures that new coins do not mix with the old coins are taken (countermeasure against replay attack) and then, after all the ledger is deleted an old coin becomes another coin (fork coin).
- 2 Empty mining can be done.

In order to record transaction information, "mining" is performed at a stage when the number of transactions has accumulated a certain amount, but in a situation where there is almost no transaction, it may take a huge time to record transactions. To avoid this, mining may be carried out even if the number of transactions is not sufficient when a predetermined time passes. This is called "empty mining". As a result, a large amount of coins significantly exceeding the required amount will be distributed, impairing the value of the coin itself.

Even now that many problems are pointed out, the enthusiasm for the crypto currency continues. While countries around the world are strengthening regulations, new coins that have cleared strict standards are being born one after another. Currencies issued only by governments or government-approved banks so far are issued by the private sectors and managed by the private sectors. There is no central administrator, and all participants equally take on the benefits of money and are responsible simultaneously.

The ideal part of the experiment called a blockchain is still moving people's heart. Because of vulnerable cryptographic techniques, theft occurs frequently, mass copies of large ledgers are difficult to mass replicate, even if it turns into a tower of Babel that requires huge amounts of electricity and communication volume, the future map produced by blockchains and coins has not lost its fascination yet. All you need is a crypto cash that does not require the ledger that humankind dreamed of once in the 1990s, and it is a completed cryptographic technology that makes a dream come.

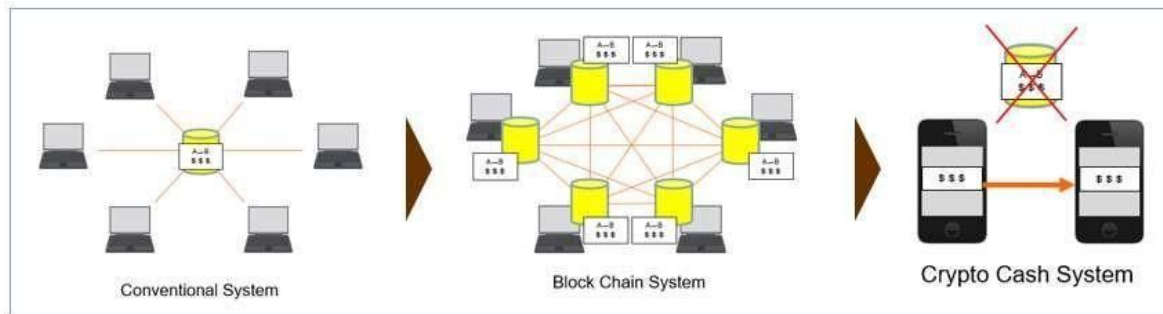
(What is “Crypto Cash”?)

"Crypto Cash", the world's first crypto cash, is a currency that uses a symbol string as a pseudo tangible material (or entity) as a substitute to be exchanged when exchanging value, and as the cryptographic technology is completed, it was developed for the first time in the world as basic technology to issue legal tenders. Information of issuers and value of cash is uniquely associated with a completely encrypted symbol string, and this fact makes tampering, counterfeiting, false use impossible. By encrypting conditions such as credit information, usage conditions, interests, deadlines, crypto cash with various functions can be created. Since it is easy to send / save electronically, it can be issued as crypto metal money or crypto banknotes if it is engraved on metal or printed on paper because it does not matter about the recording medium. As with conventional currencies, since it has entity of symbol string, it has three basic functions of "means of settlement", "means of storing value" and "value scale" as real cash. A crypto cash can be issued as a legal tender based on state credit as well as metal or paper based currency or as a convertible ticket with another legal currency, but it can be issued by issuers such as banks or global companies as in Hong Kong, or issued by community group with its credit. As a guarantee of trust, it is considered to issue not only with the value of precious metals such as gold or silver, but also with the value of natural resources as collateral.

In the first place, cash is a substitute that can exchange value indirectly, so it is sufficient for consensus to be taken between the two who are the smallest unit of value exchange. It is possible to exchange value by exchanging worth (or credit) or mutual trust with the substitute which uniquely corresponds. Or by exchanging the value guaranteed by the custodian (or credit provider) with the substitute which uniquely corresponds. For this reason, most of current cashes are issued in advance with the issue quantity and schedule determined, and generally the country or central bank distributes cash to the market while storing and managing it. In the case of crypto cash, substitution is simply an encrypted symbol string and it is nothing different from conventional money. It cannot be counterfeited or fake use, and it is a better substitute with an unprecedented feature of not selecting a medium. Crypto cash is usually issued as a legal tender with the country's credit (national strength). Or with the credit of previously issued legal currency and natural resources.

As shown in the figure below, all data such as currency information was conventionally stored, calculated and managed in the central server, but with the advent of the blockchain, the system evolved into a system that looked equal at first glance, where all nodes (servers) duplicate and own all the data. However, as mentioned above, it is about to collapse due to

vulnerable cryptographic technologies and fundamental defects. On the other hand, a crypto cash is a one-on-one value exchange system, and every crypto cash does not need a ledger at all. As with current cash, transferring value directly is done by taking out cash from the wallet handing it to the other person.



(Current Coins and ICO)

In the first place, Bitcoin has been recognized and valued in the community of all people participating in this attempt as an experimental trial. Currently, only coins with market capitalization exceeding 1 trillion yen (as of February 25, 2018/1 dollar = 107 yen conversion), Bitcoin (BTC), Ethernet (ETH), Ripple (XRP), Bitcoin Cash (BCH) and Light Coins (LTC), and more than 1600 coins have been reported.

Taking an example of a Bitcoin with the largest market capitalization as an example, it requires an extra commission and it takes more than 10 minutes to store the transaction record to a blockchain, so it is not practical, but theoretically it is possible to settle, so it is sometimes treated as "currency like". However, considering the three functions of "means of settlement", "means of storing value" and "value scale", it is insufficient as a settlement function, and the value scale since the relative value with other legal currencies fluctuates wildly. Similarly, it is thought that it is also dangerous as a means of storing, and it is never recognized as a currency. In many countries it is considered a commodity (a commodity subject to futures transaction). Unexpectedly, the volatility of value to other currencies recognized by other communities became fascinated as speculation subjects. It was bought as the target itself of speculation that is worth more than simply holding it. However, when Chinese government prohibits it in September 2017, coin exchange shops which had acquired Bitcoins by Chinese yuan, which was mostly used to exchange until then, sold their Bitcoins until next January with the price operation. After they released all mostly to the ordinary speculators who used Japanese yen, the value has steadily lowered, and now it is in a state of lull.

What is valuable only in the community of the participating members, that is a token/coin. Either local community, company, volunteering circle, anyone can issue tokens/coins. Even if it is worth for a community, it is not necessarily worth for other communities. The exchange of each token/coin beyond the boundaries of the communities is presumed to be based solely on the power relation to the market quotient of the community and there is no ground for anything.

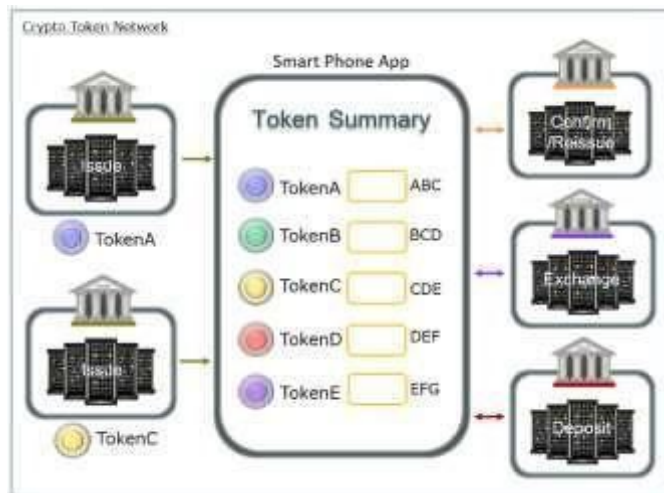
As mentioned, various coins have been issued. But when people began to think that the act of issuing coins was close to the company's public offering and to call it ICO (Initial Coin Offering), companies and organizations started to use ICO for the means of raising money. Tokens/coins with this new specific purpose are often called tokens/coins. In the first place, these tokens/coins are issued as tokens/coins of an existing coin platforms such as colored coins (in the case of Bitcoin) of existing tokens/coins. As mentioned, tokens/coins have

been differentiated into two, tokens/coins themselves and tokens/coins like corporate bonds for raising funds. Although the latter will be subject to various restrictions in the future, it seems that it will be recognized all over the world as the latest funding methods. Token/coin issuers should increase the value of services for the acquires of tokens/coins and should fascinate more participants to the community. Token/coin issuers, it is important that many people join and make vigorous communities by making even a little more valuable token/coin. In short, it is important to enrich the community and contents.

(Coin evolves into Cash)

For the development of tokens/coins, the tokens/coins themselves as platforms must develop steadily. But as mentioned before, the Tower of Babel is beginning to collapse. It is a situation at the tokens/coins themselves can be said to be castles on the sand.

The collapse of the token/coin platform using a blockchain has already begun, and the provision of an alternative platform is awaited. Traditional blockchain type token/coin platform has been subjected to repeated improvements, but it is known that structural defects cannot be overcome, and what is drawing attention as the most promising candidate that can solve this problem fundamentally is a Cipher Core Platform based on crypto cash technology. Regarding tokens/coins already issued based on blockchain platforms, much of what the community wants to keep will be changed sequentially to the token/coin issued on Cipher Core Platforms.



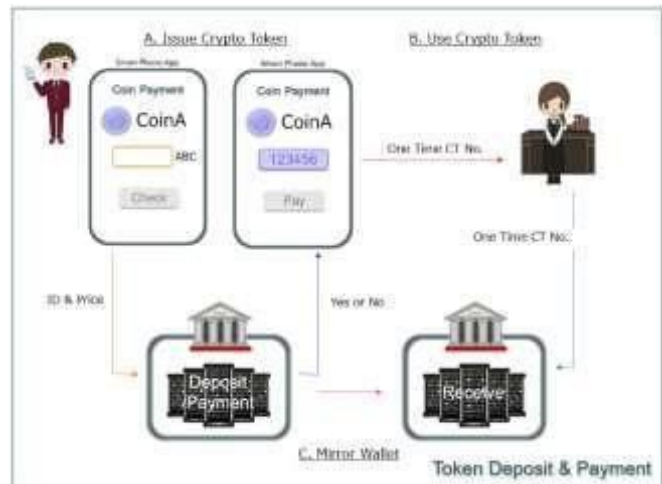
As before, a token/coin is issued by the representative of the community with the rules such as token/coin name (token/coin symbol), token/coin total amount management (increase / decrease) function, token/coin management authority setting, token/coin exchange (basic remittance) basic function and etc. As with conventional cash, tokens/coins have the entity of a symbol string and are used for "settlement", "exchange", "storing", and so on. On Cipher Core Platform consists of a user application (Wallet) provided on such as smartphones and four functions dedicated to the community issuing each token/coin; ① token/coin issuance function, ② token/coin confirmation / reissue function, ③ to large units or small units exchange function, and ④ token/coin lending box function, and the Cipher Core Platform is operated by the community.

These systems cover the operating expenses by collecting fees at the time of issuing tokens/coins, at the time of exchange of money / use, etc.

Keep the token/coin carefully so that it will not be lost like traditional cashes. If it is a large amount, you can deposit it in a place (Deposit) where you feel safe like a financial institution or a lending box. Also, if you give the token/coin to the other party as it is, you can use it for transfer or payment of money. Although it is possible to use the conventional payment

method such as QR code payment for delivery of tokens/coins, it is possible to perform settlement using a part of the tokens/coins while keeping them as shown in the figure. As an example, I will explain the method called "Six Pay" operating on the Cipher Core Platform.

After sending the amount information you want to settle from Wallet to Deposit, verifying the remaining amount, the Wallet application creates a 6-digit number using cryptographic technology, hands it over to the settlement destination, the settlement destination goes to its Deposit through the browser, then settlement is completed by sending 6-digit number. No private line (confidential communication) or dedicated reader is necessary. Since the tokens/coins are kept in a safe place, it reduces the risk of loss, and it is possible to save time and cost for exchanging money when the token/coin in hand is not exactly the settlement amount. From now on, this Cipher Core Platform will also be applied to traditional stocks (crypto stock) and bonds (crypto bond).



(What is the key cryptographic technology?)

Historically, cryptographic technology has two problems as the problem of integrity of the cryptographic algorithm (proof of undecipherability) and transfer of cryptographic key.

The completeness of cryptographic algorithms is to mathematically prove that ciphertexts encrypted with complete algorithms can never be decrypted when there is no cryptographic key.

Once Father Claude Shannon, father of information theory, in his paper published in 1949 "Communication Theory of Secrecy Systems", introduced the Vernam cipher (onetime pad cipher) and proved mathematically that it is "unbreakable". However, it is difficult to create a completely random number equal to or longer than the main body of the message, it is difficult to properly manage it, enormous time and cost are required, so it is not generally used.

In addition, in the common key system using the same encryption key for encryption and decryption, the encryption key transfer problem is to safely deliver a common encryption key from the encryption side to the decryption side. Although the public key system and the public key infrastructure that developed based on it have been widely used as solving key transfer problems, it is pointed out that in reality there are serious vulnerabilities. It has also been found that even with the use of Quantum Key Distribution (QKD), which is said to be the ultimate crypto system attracting public attention, it cannot prevent man-in-the-middle attack.

As information communication becomes a fundamental infrastructure of society, quantum computers that can handle huge calculations in extremely short time have been developed, and it is now becoming a reality to decipher the conventional encryption in a very short time. In the near future, cryptographic technology that overcomes the above two problems is indispensable, u-VKS is the first cryptographic technology that solved both problems, and it is the basic technology used for CIPHER CORE.

(Outline of Token)

Name: CIPHER CORE

Abbreviation: CIPHC

Total issue number: 200,000,000 pieces

System: Ethereum ERC 20

(Outline of Future Released Token)

Name : CIPHER CORE CASH

CASH

Abbreviation : CIPHC

System : NCC20

Crypt Type : NTI-CORE Ver.5.0

Total issue number : 200,000,000 pieces (Changeable)

Mining: None

(Roadmap)

Listing:

Starting from listed on KeY Exchange at Macau on December 16th, 2018.

Development:

Cipher Core Platform will be completed around March 2019 and CIPHER CORE will be exchanged to CIPHER CORE CASH based on our new platform.

(Use for procured funds)

- 1 50% to be sold at the exchange market or outside of us.
- 2 50% to be maintained at our side.

<Usage of the fund to be sold to the outside>

- Covered initial costs set up
- Development of various systems and engineering costs
- Reserve for market making to stabilize the price of coin/cash
- M&A and alliance costs with the outside organization and outsourcing

(Directors)

RYOICHI TAGA (CEO)

Experience building systems such as digital signage, video distribution, online game, etc. After that, he also worked on the development of the FinTech field.

He supports research and systems in the AI field at the University of Tokyo.

He is interested in the crypto currency field for a long time and is developing and researching systems.

TAKATOSHI NAKAMURA (CTO)

Ocean Engineer in the Department of Ocean Engineering at Massachusetts Institute of Technology.

Science Master's degrees in Department of Mechanical Engineering and Civil Environmental Engineering at Massachusetts Institute of Technology.

After working for McKinsey & Company, he joined Massachusetts Institute of Technology as a research affiliate and researched in future production, artificial intelligence and information security. And he completed crypto technology and developed crypto cash technology which will be final currency form of cash.

He is now CEO of NTI, Inc. and Director of Japan Society for Security Crisis Management.

HIDETOSHI ITOH (DIRECTOR)

Current Position

- (UAE) CEO, Bonj Consultancy International (Investment Bank and Consulting)
- (Estonia) CEO, Aplotech, Crypt Currency Exchanges
- United Nations International Police Commission member
- Executive Advisor, Jupiter Project、Stanford Cyber Initiative, Junca, etc.
- (UK) Executive Chairman, Zufi Alexander Inc. (Best Fashion Brand Award in UK, Paris Collection)
- Doctor of Humanities

Biography

- Management Science, Master's and Ph.D program, Stanford University, Research Assistant
- McKinsey & Company (Management Consulting)
- IBM (R&D, IBM Certified Professional、Corporate Venture Capital Committee member)
- COO, UL SYSTEMS (JASDAQ)

- Executive Management Director, Future (TSE #1)
- Committee Member, Japan Association of Corporate Executives (JACE, KEIZAI DOYUKAI)
- (London, UK) External Director, Future System Consulting UK Ltd
- Executive Vice President, CFO & CSO, Forval (TSE #1)
- CEO, Forvalive
- Visiting Professor, Graduate School of Business (MBA course), Waseda University
- Advisor, Och-Ziff Capital Management (Hedge Fund, New York Stock Exchange)
- External Director, Livedoor Holdings (M&A, Turn Around)
- Senior Advisor, Olympus Capital (Private Equity, New York : Kyoto Kimono Yuzen, Arista, etc.)
- Executive Chairman, Soho's Hospitality Group
- CEO, dna Model Management Japan (World's No.1 Fashion Model Agency)
- (BVI, UK) Co-CEO, Japan Entertainment Corporation (Macau, Casino 5-Star Hotel)

(Disclaimer)

This white paper is intended to provide information and is not intended to promise any contract provision. It is not intended for individuals and corporations in countries / areas forbidden to sell and purchase similar coins by law.

In case that token/coin may be regarded as a security, the US securities law may be applied. Investment in the same coin is restricted and banned in the United States except for some investors to comply with the law. Please confirm SAFT or JSAFT (in case of Japanese) separately for details.