Dark Cash(XDC)

Dark Cash (XDC) is a coin that has made a big change in the dark market for 19 years, originating in Canada. The Dark Web is often perceived as unfamiliar in a market that can not be heard at first glance. That should be the case, and illegal trades such as “firearms, viruses, cannabis etc.” are being made on a daily basis on the market.

But that doesn't mean that it doesn't matter to everyone who is looking at this at all. The fact is that the actual demand for cryptocurrency is still large on the Dark Web. The history of cryptocurrency is no exaggeration to say that it is the history of the dark web. The rise in price of bitcoins has been achieved by the evolution of the dark web.

If we look at how much the transactions on the Dark Web made a contribution to the soaring bitcoin, we think we can see how important it is to hold down the market.

First of all, you will understand what the dark web is.

Basically, Internet sites can be broadly divided into three.
1. Surface Web This is a site that can be viewed from a general search engine, such as Yahoo! or Google.
2. Deep Web (Deep Web) Search Engine, Member Limited Page, SNS Login Screen Basically, you can enter an ID and password, and then you can recognize that the page you visit is that.
3. Dark Web A web site that can only be viewed under special circumstances, and full confidentiality is guaranteed.

The Darknet website can only be accessed through networks such as Tor ("The Onion Router") and I2P ("InvisibleInternet Project").
Darknet's identity and location remain anonymous and can not be tracked.
Darknet encryption technology routes user data through a number of relay servers to protect identity and guarantee anonymity.
Therefore, communication between Darknet users is highly encrypted, enabling them to secretly share conversations, blogs, files, etc.
Therefore, it is said that it is difficult to be arrested because the secrecy of illegal transactions is also widespread, even in many cases.

And the net which does not have the anonymity which put together the surface web and the usual deep web (private page which needs authority) is collectively called " clear net ".
Of all the sites on the Internet, the percentage of Clearnet is actually said to be " 1% ". In other words, there is a fact that most of the Internet exists in an environment where you can not usually access it. The economic effect, the market size is out of the ordinary, the coin check incidents and numerous hacking incidents in Japan, Marriott, Facebook, Amazon, credit card information theft etc. It is no exaggeration to say that it is being traded.

Big pillar supporting bitcoin

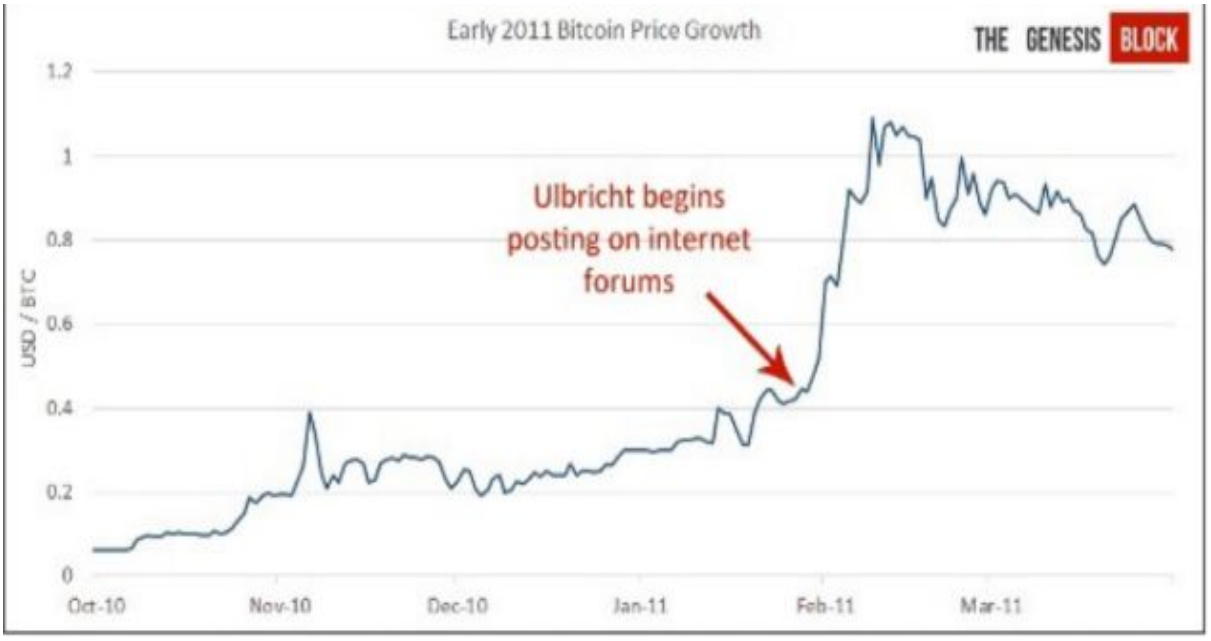
Next, let's get closer in time series on how these sites are big pillars to support Bitcoin.

Six years ago, it was 1 BTC = 0,000776.
September 29, 2008 Stock Price Plunged
January 3, 2009 Birth of Bitcoin
February 6, 2010 First Bitcoin Trading
May 22, 2010 Purchase Pizza at 10,000 BTC
July 2010 Exchange Value 10x
January 1, 2011 (Dark Web) Silk Road will be launched
March 6, 2011 Mount Gox sold
April 2011 1 BTC = 1 EUR
September 27, 2012 Bitcoin Foundation established
February 22, 2013 1 BTC = 30USD
March 21, 2013 1 BTC = 75 USD
March 28, 2013 Bitcoin market capitalization reaches $ 1 billion
However, since Silicon Valley has entered, August Bitcoin's ruling with the currency fell sharply.
August 6, 2013 Bloomberg Displays Bitcoin Chart
November 2, 2013 1 BTC = 200 USD
November 7, 2013 1 BTC = 500 USD
November 25, 2013 $ 1 million btc is stolen.
January 27, 2014 Charlie Shrem is arrested on suspicion of ML.
February 15, 2014 Mount Gox broke down

The largest market ever symbolized in the Dark Web and Bitcoin is the " Silk Road " with more than one million users.

In fact, Bitcoin has grown a great deal when it began to post Silk Road forums and sites, and as of 2011, the media recorded a silk road more

than 100 times in half a year when it was covered However, prices continued to grow.



In addition, as the Silk Road received DDos from 4/24 to 5/1 in 2013, Bitcoin fell by more than 40%, and the market is now firmly supported by the darknet for most of Bitcoin's growth I am keenly aware of what I have been doing.

It can be inferred from many records like this that the Silk Road has been greatly influenced by the formation of Bitcoin.
Actually, however, the Silk Road closed in 2013 is only the beginning, and as you know, the real breakthrough of cryptocurrency was from here.
Silk Road 2.0, 3.0, 4.0, and more than 400,000 users were said to have been there even after the closure of the Silk Road Alphabay, evolution, and DREAM Market headed the market like a flood after the rain, and a bit more in line with it We push up the price of the coin and it reaches to these days.

behind story of Bitcoi

Next, I'll tell you a lot of misunderstood " Bitcoin Birth Secrets ".

In fact, Bitcoin is a thing that was made to " to be completely hidden and to trade.
There was a thought of some thinkers called " Scipher punk ".
Of course, "Sashinakamoto" also had the idea of being located in "Cipher punk".

'Design an electronic financial system that does not allow third parties to intervene. " By Sashinakamoto

In the past, when sending money, exchanging with other currencies, the existence of an intermediary, such as a payment service or a bank, was essential.
In fact, mining is dominated by large organizations with power, but it works naturally. Bitcoin was created by Cipher Punk. It is a group that aims to build a new Internet world using cryptographic technology.
In recent years, it is no exaggeration to say that all communications over the Internet are intercepted by government agencies.

"" Only outlaws have privacy "

That's their message. Confidentiality of payment was essential in true democracy.

Only a few programmers, such as cryptologists, were involved in Bitcoin in the early days.
But that changed on the Silk Road, which was founded by Rosulbricht. It was a dark market where any deal could be done on the dark web.

Since the settlement there was anonymous Bitcoin was most appropriate, he incorporated the system.
That triggered hundreds of thousands of dollars in price.
Of course, the presence of Bitcoin also flew across the United States on the ground in the blink of an eye.
Citizens are free to create markets and trade without surveillance or regulation.
After a number of scandals, trading volumes declined but recovered quickly. The bad thing is that the user did not miss the essence of being a black market, not Bitcoin. In reality, bad things happen more often with cash transactions.

Darknet's amazing market size

The market size of funds flowing on the Dark Web is said to be more than 100 billion dollars in the US dollar alone.
In addition, it is said that the cryptocurrency brought in from the Clearnet to the Dark Web in 2017 will be worth more than $ 10 billion, and its circulation amount surpasses any existing exchange.

Currently I am obscuring the name here, but the categories traded in going to a large market are

- Illegal drugs such as cannabis and cocaine
- Legal drugs prescribed by a doctor
- Dangerous goods such as firearms and explosives
- Extreme videos such as child pornography and murder videos
- Hacking agency and sales of viruses
- Personal information such as forged credit cards and passports

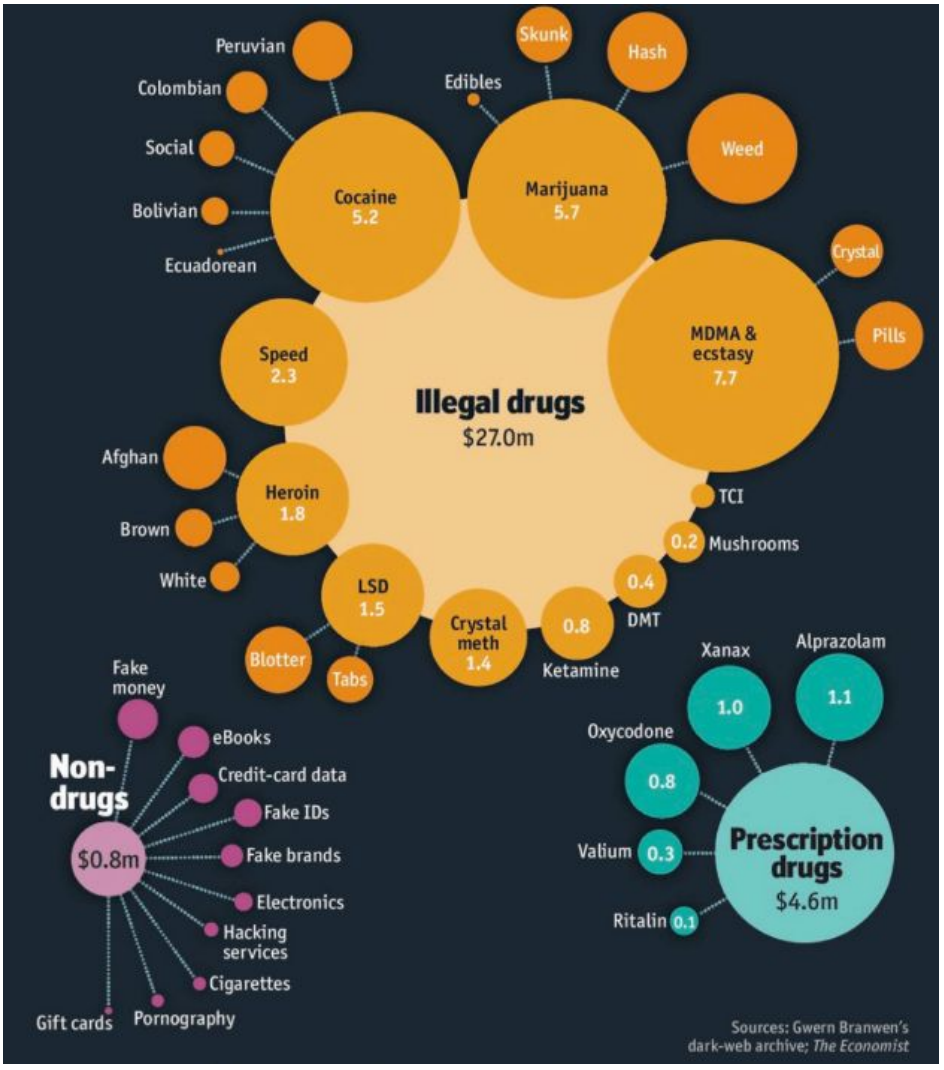
But of course, there are many regular services that are sold on Clearnet.

Among these, hemp is one of the current topics in medicine.
So why is the turnover of cannabis soaring?
Why we pay particular attention to cannabis and start activities centered on Canada is a strategy that also considers legal risk.

Why Marijuana Market Is Larger Than Other Transactions

In the case of international trade, illegal trade will bring considerable risk to each other, but if it is legal, merchants will enter the demand in the illegal country in a crying manner.
In other words, cannabis that has a mixture of illegal and legal countries has a much higher turnover than firearms and stimulants, which are categories that both countries are likely to be illegal.

Cocaine is heterogeneous, and it still has a large sales volume mainly in the US area due to the presence of a large sales channel from El Salvador and Nicaragua via Miami. However, the cannabis market is popularized globally.
In Canada, cannabis was legalized the other day.
In other words, our project will be able to act legally in the country.
In fact, there is no problem with activities such as XMR, ZEC, LTC and DASH, and the market capitalization continues to increase. Let's look at the actual turnover.



Here is a sample of trading volume that picked up some dark markets of a certain year. The actual turnover is expected to be around 5000-8000 times.
Please check it as a document for ratio determination.

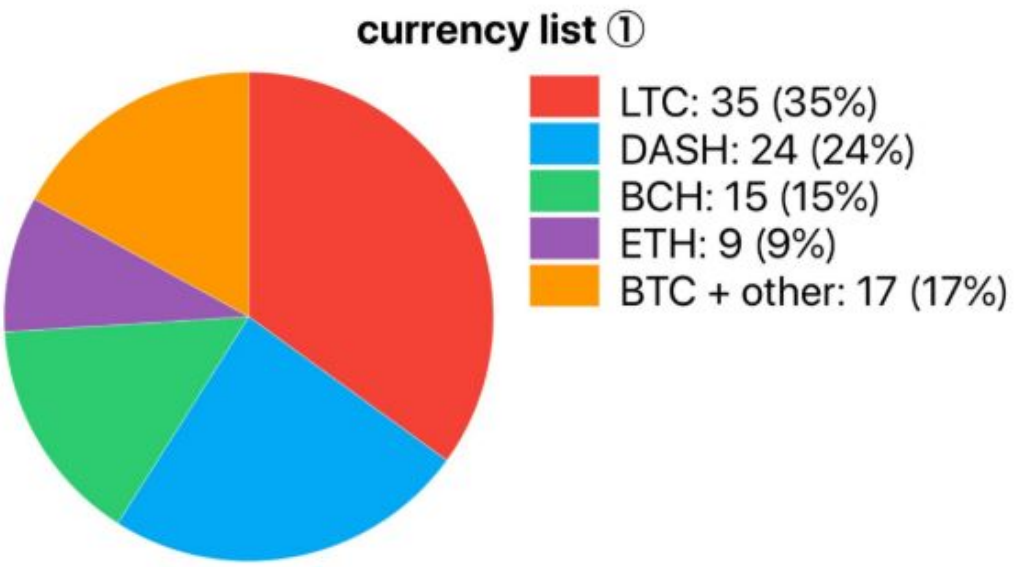
Drugs 31, 6 (illegal 27: legal 4, 6)

Other than that, it can be seen that this has an overwhelming share of drugs, with 0,8. In recent years, tumbling and cashing services for cryptocurrencies have been steadily increasing.

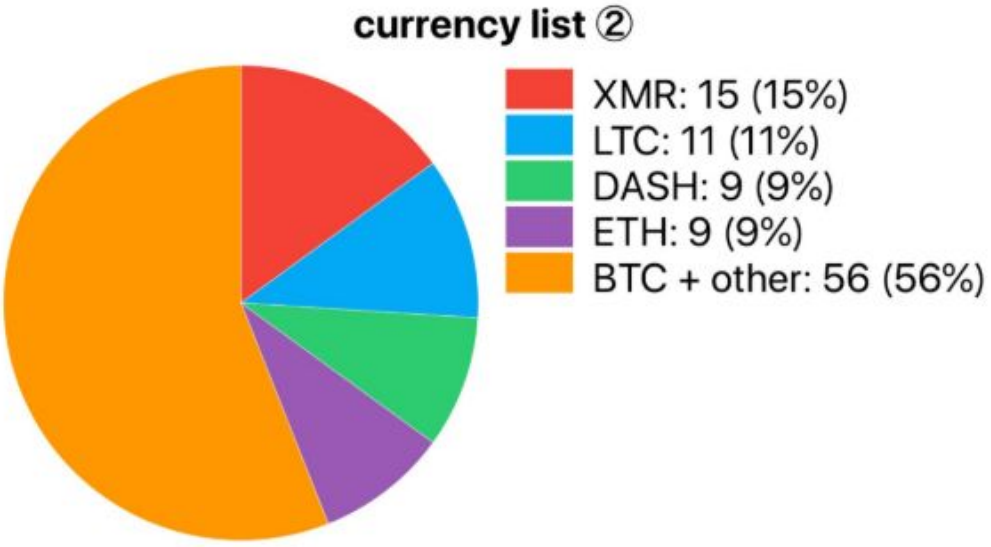
The dark market and bitcoins that have raised bitcoin prices hundreds of thousands of times now

Trading in the dark market is still popular today.
Nowadays, there are many types of blockchains, and more anonymity-focused currencies have been issued, such as not displaying transactions on blockchains.
Currency other than Bitcoin is also actively used.
Prices soared in the second half of 2017, fees increased, delays in transactions, etc., and the community began to feel the limit of bitcoin as a practical application.

Although the ratios differ in the euro area, the United States, Central Asia, etc., ETH, LTC, XMR, DASH, etc. are widely used, broadly divided.
The following ratio is considered to be one of the most powerful theories in one survey result.



In Eastern Europe, including Russia, Bitcoin was followed by Litecoin (35%), followed by DASH (24%), Bitcoin Cash (15%) and Ethereum (9%).



And all of these currencies have very high market capitalization.
ETH Present CMC Second largest market capitalization $ 0.16 trillion
LTC Presently CMC 7th largest market capitalization $ 0.025 trillion
XMR Presently CMC 9th largest market capitalization $ 9.5 billion
DASH Presently CMC 10th largest market capitalization $ 14 billion

In fact, although it should be rare to use anything other than BTC and ETH as a basis or something, it is because there is a real demand for this darknet that they are accompanied by such growth and market capitalization. It will not be.

Basis Technology of block chains

The hash function plays a very important role, such as hashing transaction information and block data immediately before in the blockchain.
By using a hash function, it is possible to make the transaction information recorded in the block a hash value of fixed size and prevent falsification of the past block.

In addition, the hash function is similar in nature to the encryption function, but the hash function has different features in that it can not be reverse calculated (it can not be decrypted).
So, here we will talk about the hash functions needed to properly understand blockchains.

▪ With one-way hash function

A one-way hash function is, in a nutshell, to “print a fingerprint of a message”.
The hash value is output by putting the input information "message" in the one-way hash function.

The one-way hash function has the following features.

If the message is different even by 1 bit, the hash value will change.
It is not possible to reverse the message from the hash value.
The hash value is always fixed size, not limited to the length of the message.
The size of the hash value is small.
Let's look at each specifically.

~ The hash value will change if the message is different even by 1 bit ~

The one-way hash function is described as "taking a fingerprint of the message". That is, if the message that is the input of the hash function changes even a little, a completely different hash value will be output.

5

For example, "sato" "kato" "Sato" to SHA-256 which is one of the hash functions described later
If you enter, you get the following hash value:

6

message	Hash value (SHA-256)
sato	60fa2fc8a5f0f8a9ea9c934350ddbe952e044aa5ba37c993da3297e4571d9733
kato	c2d59dab4f088d9bd3ce5c6d8f06a09a6623a1f6df216f959e2d81177c615b80
Sato	1b4ed9b60cc00906f43ef19f027436c2c5edb1c9652ca75e2b47126afb3962ba

In this way, if the message is different even with one character, you can be sure that a completely different hash value is output.
In hash functions it is very important to avoid hash collisions. In other words, it is necessary to avoid outputting the same hash value for different input data.

~ Not only the length of the message, the hash value is always fixed size ~

One important feature of one-way hashing is that it outputs fixed-size hash values for messages of any length. See also the example here.

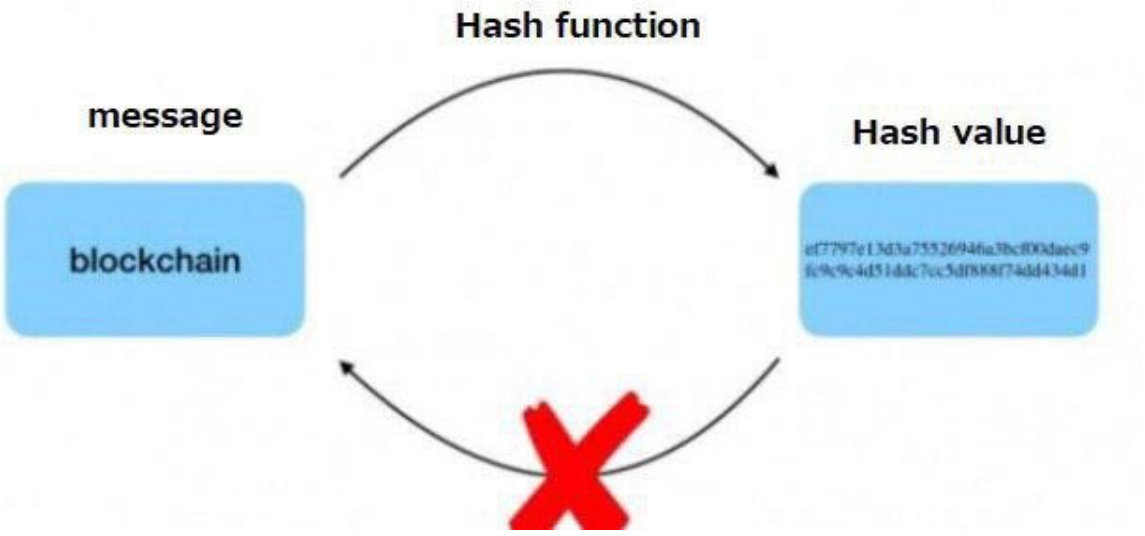
7

message	Hash value (SHA-256)
blockchain	ef7797e13d3a75526946a3bcf00daec9fc9c9c4d51ddc7cc5df888f74dd434d1
blockchainblockchain	b355873afc498146f10521780b0f18fd4fc4985c440b2efae03290dc0662da06

In this example, we can see that the size of the hash value is the same despite the difference in the number of characters in the message.

There is no big difference in the amount of data with this number of characters, but if you pass 1TB of data contained in the hard disk to a hash function, you can get a 256-bit (32-byte) hash value as well.

~ Can not reverse message from hash value ~



The hash value can be easily calculated by passing the message to a hash function. However, the original message can not be calculated from the hash value.

While cryptographic functions can generally encrypt and decrypt, hash functions can transform data in only one way.

The fact that it is designed to be a fixed size output for any input also makes it difficult to reverse the message.

~ The size of the hash value is small ~

It does not matter how large the input message size is (it has an upper limit due to the hash function), but the size of the output information hash value is reduced to be manageable.

The size of the hash value differs depending on the type of hash function.
9

Hash function	Output size (bit)
SHA-256	256
SHA-512	512
MD4	128
RIPEMD-160	160

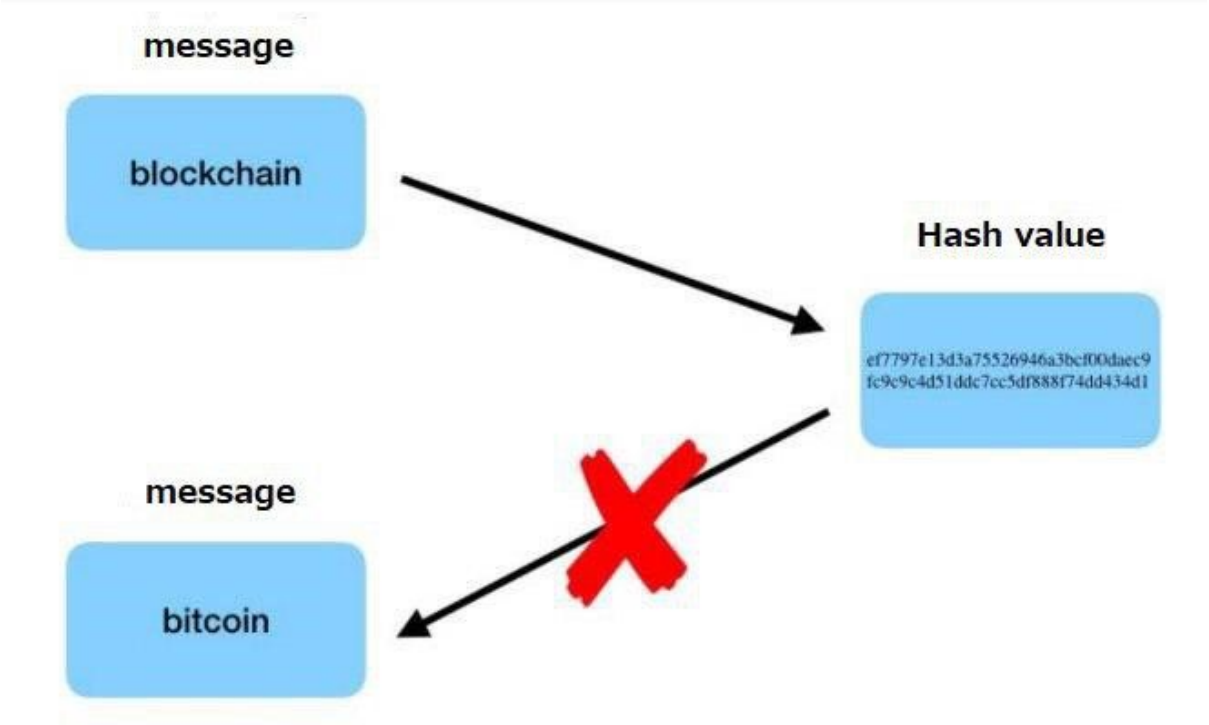
It can be understood that the ability to reduce the size by hashing a large message like this is important even in view of the limited amount of data that can be recorded in a block. By the way, at the moment, the bitcoin block size is 1MB.

~ What is secure hash ~

A secure hash function must have at least two properties: weak collision resistance and strong collision resistance.

※ Weak tolerance

10

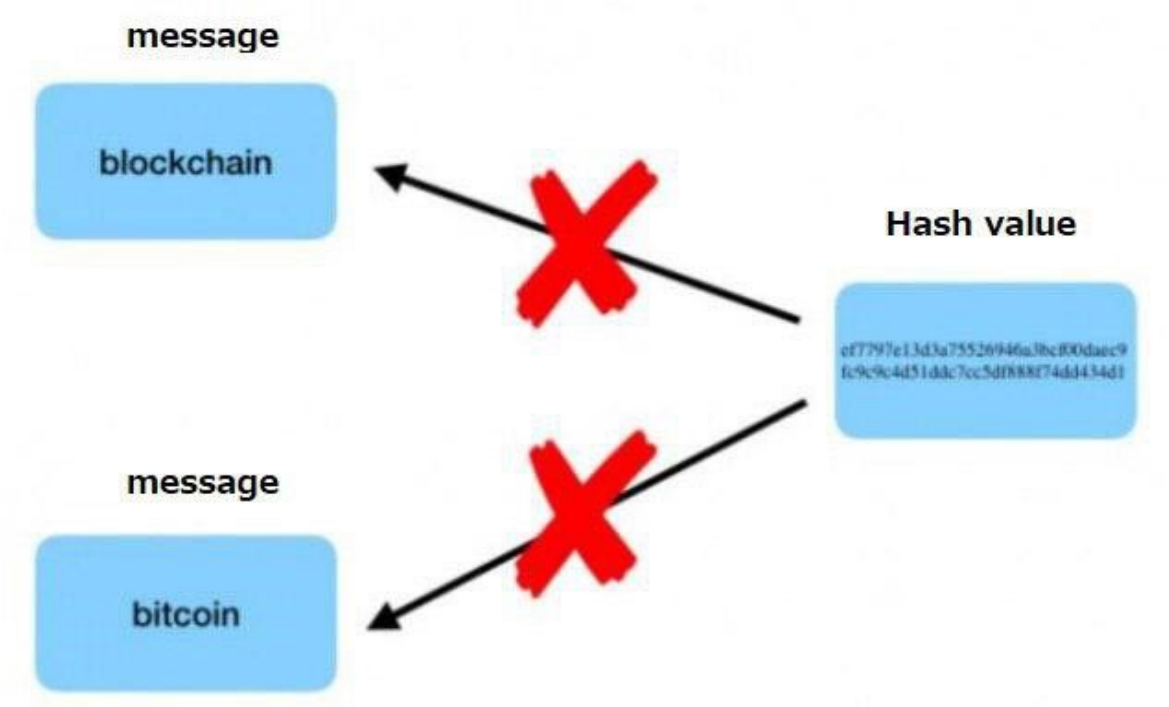


To be a secure hash function, given a message's hash value, it must be very difficult to find another message with that hash value.
This property is called weak collision resistance.
In the above example, the hash value obtained when the message blockchain is input to the hash function can not be calculated back to other messages such as bitcoin.

At the moment, hash functions such as SHA-2 and RIPEMD-160 used in Bitcoin are weakly collision resistant.

Strong collision resistance

11



Strong collision resistance is the property that it is very difficult to find two different messages whose hash values match.

In the example above, when you back calculate a hash value, you can not find two different messages like blockchain and bitcoin.

In general, strong collision resistance is more easily defeated than weak collision resistance.
SHA-2 and RIPEMD-160 have strong collision resistance, but strong collision resistance such as MD5, SHA-1 and RIPEMD is broken.

~ Hash function used in block chain ~

In the bitcoin blockchain, two types of hash functions, SHA-256 and RIPEMD-160, are used in various situations.

Bitcoin also uses a double hash that uses these two types of hash functions in an overlapping manner.

In other words, using the SHA-256 hash value as the input value of RIPEMD-160 and using the hash value that passes the hash function twice improves security.

In many cases, SHA-256 double hash is used, and when short hash value is required, SHA-256, RIPEMD-160 double hash is used.

※ What SHA-256 is

SHA-256 is a one-way hash function created by NIST (National Institute of Standards and Technology), which outputs a 256-bit hash value.
Force
SHA-256 is a kind of SHA-2, and there are SHA-256, SHA-384, SHA-512, etc. depending on the difference in bit length.

The longer the bit length is, the more the hash collision can be avoided, but in the bitcoin block chain, SHA-256 is adopted in consideration of the balance of calculation degree, easiness of implementation and safety.

There is also SHA-3, which is said to be more secure than SHA-2 in hash functions. This SHA-3 is used for virtual currency such as IOTA.

※ What RIPEMD-160 is

RIPEMD-160 is an improvement over the original RIPEMD hash function. The RIPEMD hash value is 128 bits long, while the RIPEMD-160 has a 160 bit long hash value.

Unlike SHA-2, since RIPEMD was developed in an open academic community, there are no patent restrictions.

However, the strong collision resistance of the original RIPEMD has been broken. In other words, you can find two different messages with the same hash value.

On the other hand, RIPEMD-160 is considered to be a secure hash function because it is not broken at this time.

The one-way hash function is not only used for block chains, but is a technology that is also used near us, such as one-time passwords used in digital signatures and internet banking.

Also, while hashing is only a small part of understanding blockchains, it can be said that it is a very important technology to improve blockchain security.

However, although the hash function can check the authenticity of data and detect tampering, it can not detect "spoofing".

It requires other technologies such as digital signatures to detect "spoofing".

· Digital signatures we adopt "BLISS"

BLISS signatures are classified as lattice-based signatures.

A lattice-based signature is an esoteric in mathematics called the lattice point search problem of lattice cryptography.
Is a generic term for public key cryptography based on
To illustrate the basic principles of lattice cryptography, vectors and matrices appear.
12, 13

3×2 Matrix example

$$A=\begin{pmatrix}1 & -3\\ 5 & 4\\ 2 & 0\end{pmatrix}$$

2×3 Matrix example

$$B=\begin{pmatrix}1 & -3 & 0\\ 5 & 4 & -1\end{pmatrix}$$

Second-order square matrix example of

$$C=\begin{pmatrix}1 & -3\\ 5 & 4\end{pmatrix}$$

Row vector example

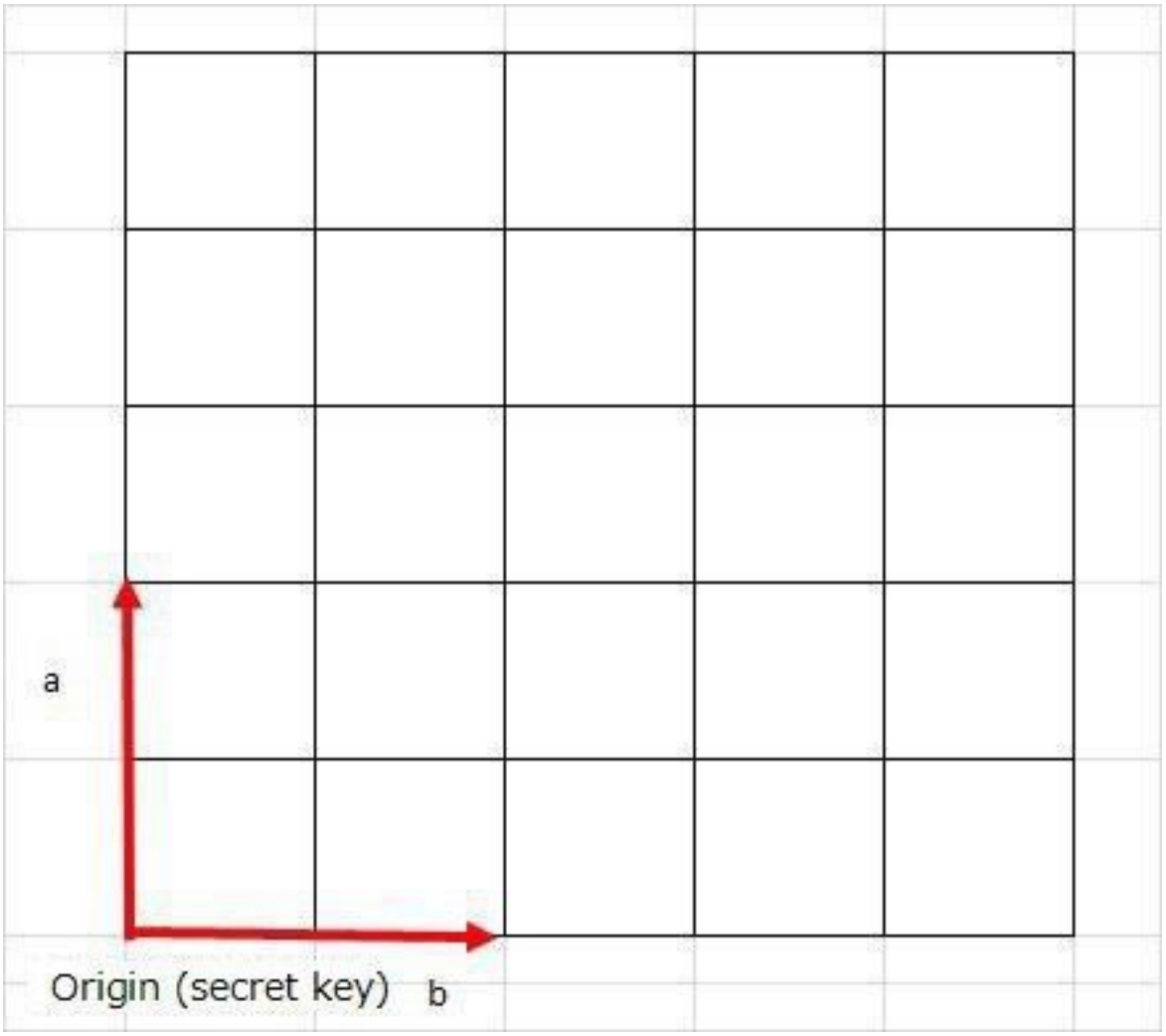
$$\vec{a}=(3,4,-5)$$

Column vector example

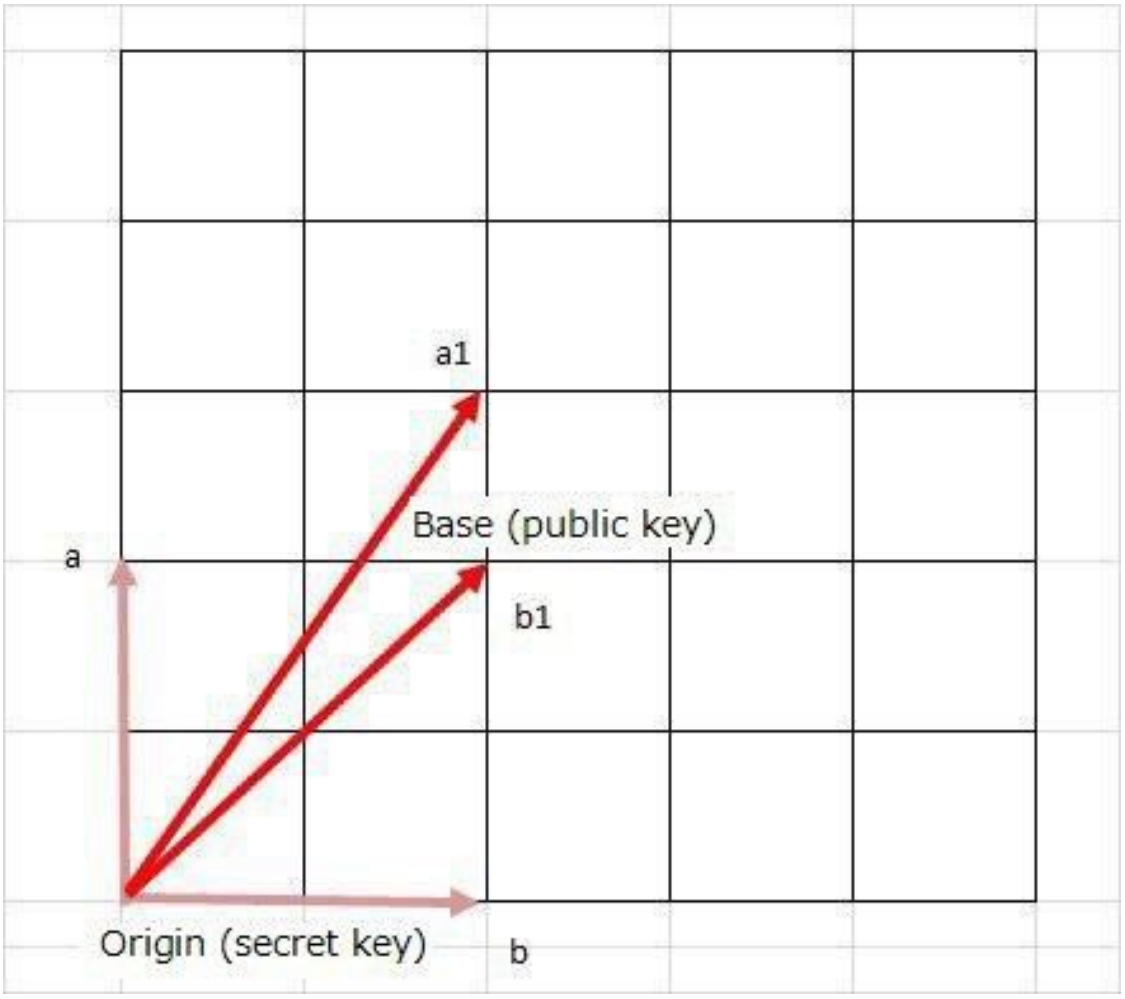
$$\vec{b}=\begin{pmatrix}2\\ -3\end{pmatrix}$$

※ Illustrates in two-dimensional coordinates for easy understanding.

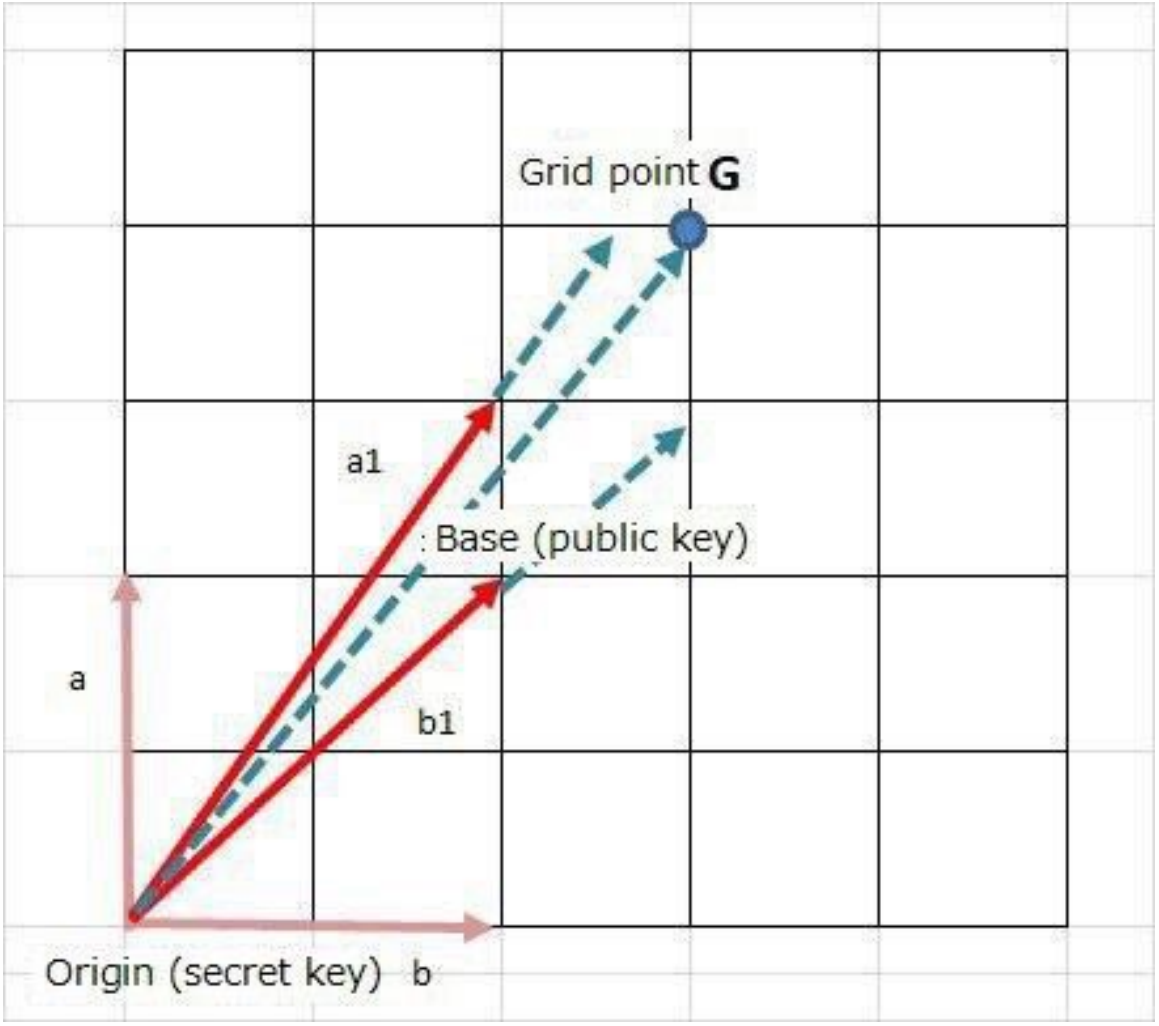
(1) A set (matrix) of points present in lattice coordinates is the "secret key".
Vectorize this.
Let coordinates (0, 1) be vector α and (1, 0) be vector β.
Since the vectors α and β are orthogonal to each other, we will call them the origin.
14



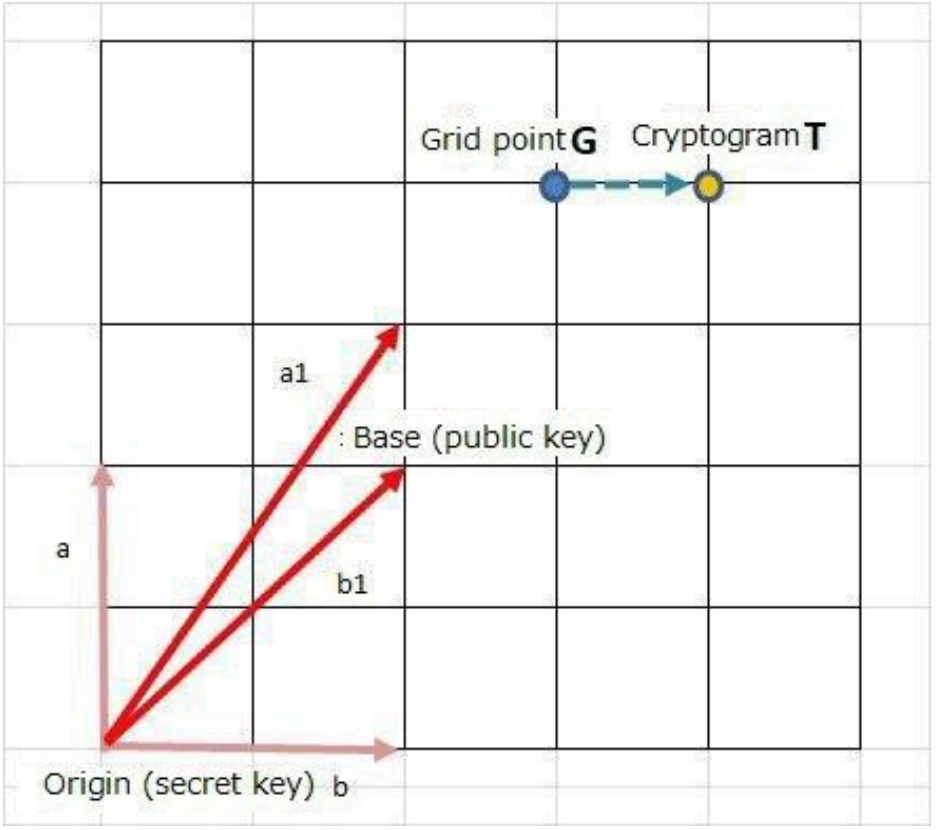
(2) A vector obtained by distorting the angles of the vectors α and β of the “secret key” and converting them into non-orthogonal vectors is called “base”.
The "public key" is a matrix of these non-orthogonal transformed vectors α1 and β1.
15



(3) To add noise to this public key (vectors α1 and β1), multiply it by m and call it a grid point G. (Calculation formula is G = m1 x α1 + m2 x β1)
16

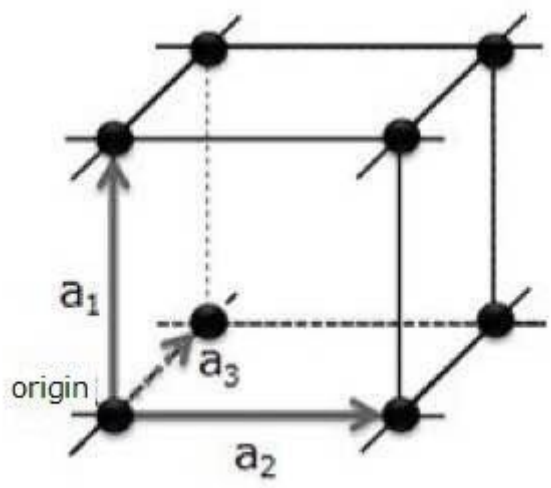


(4) By adding the vector γ to the generated grid point G
Ciphertext T is completed.
17

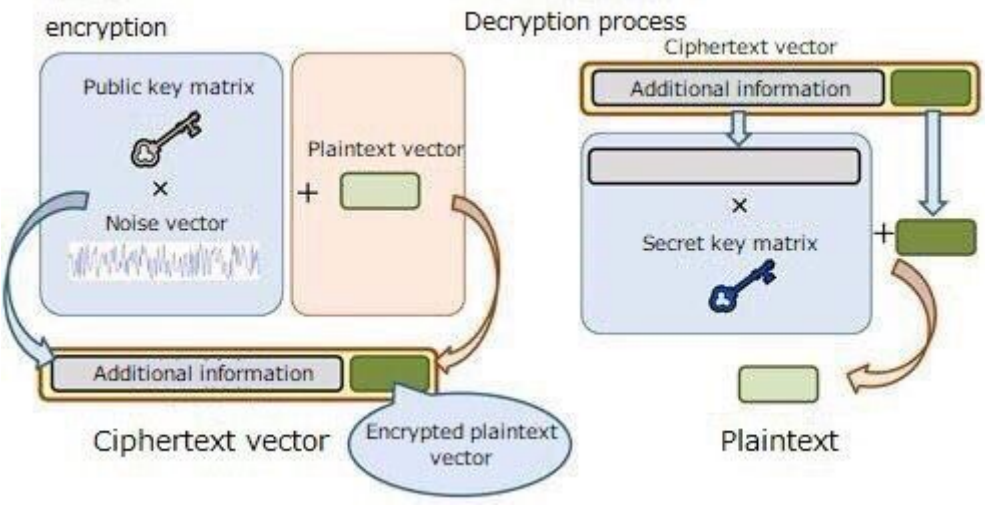


In order to decrypt the secret key from the ciphertext T and the public key, it is first necessary to find the grid point G.
In this example, I explained with a two-dimensional lattice vector for clarity, but the matrix is difficult to find the coordinates of the lattice point for encryption in vector calculation in three-dimensional and multi-dimensional as follows The degree is much higher.

And finding a grid point is even more difficult to get to the secret key.
18



A digital signature that uses the above lattice code is called a "grid-based signature".
The operation of encryption and decryption processing of "lattice base signature" is as follows.
The noise vector is "grid point G" mentioned above.
19



what about our cryptocurrency

Dark Cash (XDC) is a coin used in the dark market, and the raised amount is capped at 1,000,000USD.
As soon as it is launched seven months later, it will flow to seller groups in each major market and will have a market capitalization of $ 10,000,000 within one year.

Ultimately, we aim for a 10% share of trading in this market.
Token name Dark Cash
Standard ERC20
Contract address 0x305955eeb8842966077e8Db03B07658926B14266
Symbol XDC
Number of digits 18
Pre-round price 1XDC = 1USD
Pre-round raised amount 1,000,000USD
Maximum issue number of sheets 3,333,333 XCH
HP http://darkcash.net/

・Road Map

2017 Fourth quarter
・project start
・Market Research

2018 Second quarter
・Technical Feasibility
・Business strategy

・Assessment by each Professional

2018 Fourth quarter
・Advertising activities
・Credit Bit partnership

2019 First quarter
・Token making
・Pre sale start
・Hard cap 5M $ clear

2019 Third quarter
・Listing Exchange
・Main net α version testing

2019 Fourth quarter
・Practical start
・Target price 10$

2020 Top quarter
・Blockchain High speed Update
・1Block = 1 sec processing

2020 the second half of year
・Digital signature ‘’BLISS’’
・Transaction Encryption

・Fands allocation

Marketing & Business (listing EXCHANGE) 25%
Platform & Technical development 45%
Reserved Fands 20%
Working capital 10%

Create a more legal anonymous trading platform

So far,
1) The general use of Tor developed by the U.S. military has been released and its secrecy has been exploited to make up the black market.
2) Bitcoin is used at the center, and the market capitalization has been greatly improved by this
3) In recent years, the market share of the trading currency has changed significantly due to the development of new and superior cryptographic technologies, and the market capitalization of the currency has been greatly successful in business due to real demand, and the investment effect has also been large. Working point
4) Basic technology of block chain
5) Digital signature scheme of cryptocurrency we announce
6) New market development by it

I have talked up to

From that, we have the ultimate goal of creating a more legal anonymous trading platform.

Up to this point we have approached business growth and return on investment.
From here, we will discuss how to use and work on the presence in the market where we are developing.

Our ultimate goal is
・Construction of environment where more anonymity is secured on the Internet
・Sound the market that is currently realizing it
It is located in

In order to realize this, the future of the anonymization of the market currently operated by Clearnet is not in the future, but in the market where the secrecy has been realized.

Through this cryptocurrency, we aim to gain a large share of usage in the Darknet market and to launch new markets with its funding sources and influence.

Many large dark market operators are said to have earned hundreds of millions of dollars.
This project will use the funds for the soundness of the industry to make the secret network more familiar to the public and help further the market development.