CUBE
CHAIN

Cube Chain

Technical White Paper

Contents

Cube Chain Technical White Paper

Cube Engine Version 2.0

1. Overview

1.1 Overview

Blockchain is an encryption system that creates blocks of data at regular intervals and validates data through hash values that are encoded within the blocks. It is a system that stores the recorded data on a distributed server. It is a system for securing the trust and the reliability of data by separately storing encrypted data along with verification data.

Compared to the existing database, the advantage of the blockchain is that it is irreversible because data is encrypted in chronological order. By sharing and storing the same data in a P2P process, data can be highly protected and maintained. As the blockchain is used as the technology for digital currency, it should gain the trust of a number of users. It is now the base technology of today's cryptocurrency market for various reasons. Although the blockchain has broken new ground in new technology by using encryption and P2P communication to create a unique technique to record data, there are still technological limitations.

For the blockchain to replace the existing database, it must be accompanied by the technical features that the existing database has, including improvements in velocity and ease of use. If the blockchain technology continues to evolve and becomes substitute for databases, it will be a very secure technique to record and manage data. In that sense, Cube Chain has used the database as the base structure for the expansion of its functional elements, instead of utilizing the block.

Therefore, it is possible to utilize several advantages of the database, which is based on the existing blockchain. The development of Cube Chain will utilize the base technology from the advanced blockchain to issue cryptocurrency and introduce various online services that require access to the public databases.

1.2 Basic Information

Cube Chain (QUB)

Coin name: Cube Chain
Total number issued: 12 billion
Algorithms: SHA256, CH-S1, CHF, SHA384
Compensation technique: POH (Proof of POW+POS hybrid)
Condition of participating in POS: should have at least 5,000 or more of Cube Chain in the wallet
Development start date: January 2017

2. Features of Cube Chain

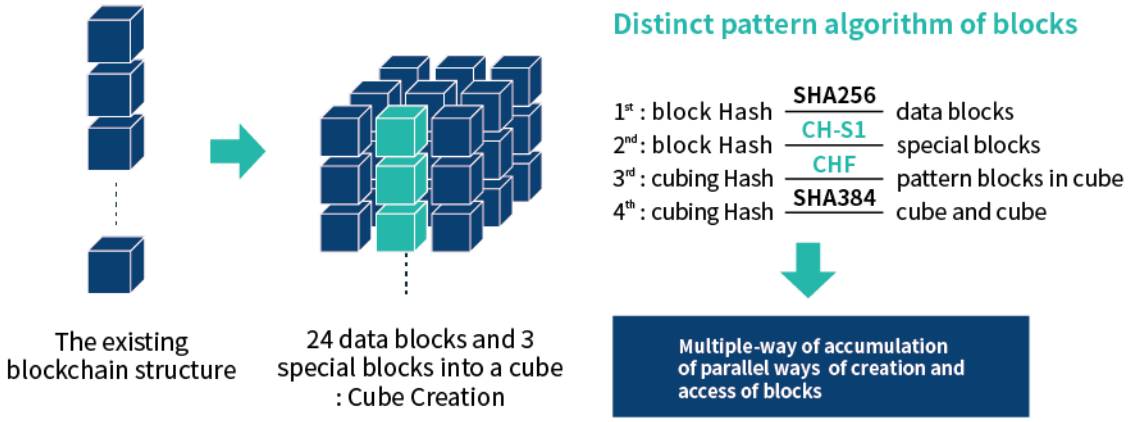
First, hash, which is the core of blockchain is the term used for encryption technology, and is described below. SHA256 is a type of encryption hash. Hash means “the act of converting specific data into data of the same length that represents the actual data.” As the symbolic data has an ability that allows the data to be completely changed, the original data is changed only a little bit, which helps it to maintain integrity. For instance, although a hash of the string ‘A’ and a hash of the string ‘B’ have only one difference alphabetically, the results can be enormously different. For example, SHA 256, a typical hash algorithm, and always returns a different 64 digits of a hexadecimal value of 256 bits, no matter what values are input.

[Figure 1]

2.1 Cubing

Cubing refers to a technology that combines twenty-seven blocks into a single cube. Twenty-four regular blocks that record transaction ledgers, and the three to five special blocks combine to create a single cube. It is not a simple grid concept, but a technique for generating blocks simultaneously. As soon as twenty-seven blocks are created the generated cube creates a hash value. After that, all the ledgers recorded continue to make the cube and the hash value connects a cube to another cube. This creates the primary encryption by connecting blocks and the secondary encryption that comes from connecting cubes. It has much stronger encryption technology than the existing blockchain.

Although a special block consists primarily of three blocks, the special blocks allow for the adjustment of the number of and the percentage of the data blocks. As soon as the data block is created, cubing proceeds, and the generated cube creates another hash value. The cubing creates a hash value for the cube, allowing it to build a double-layered approval data with the hash value of the block.



[Figure 2]

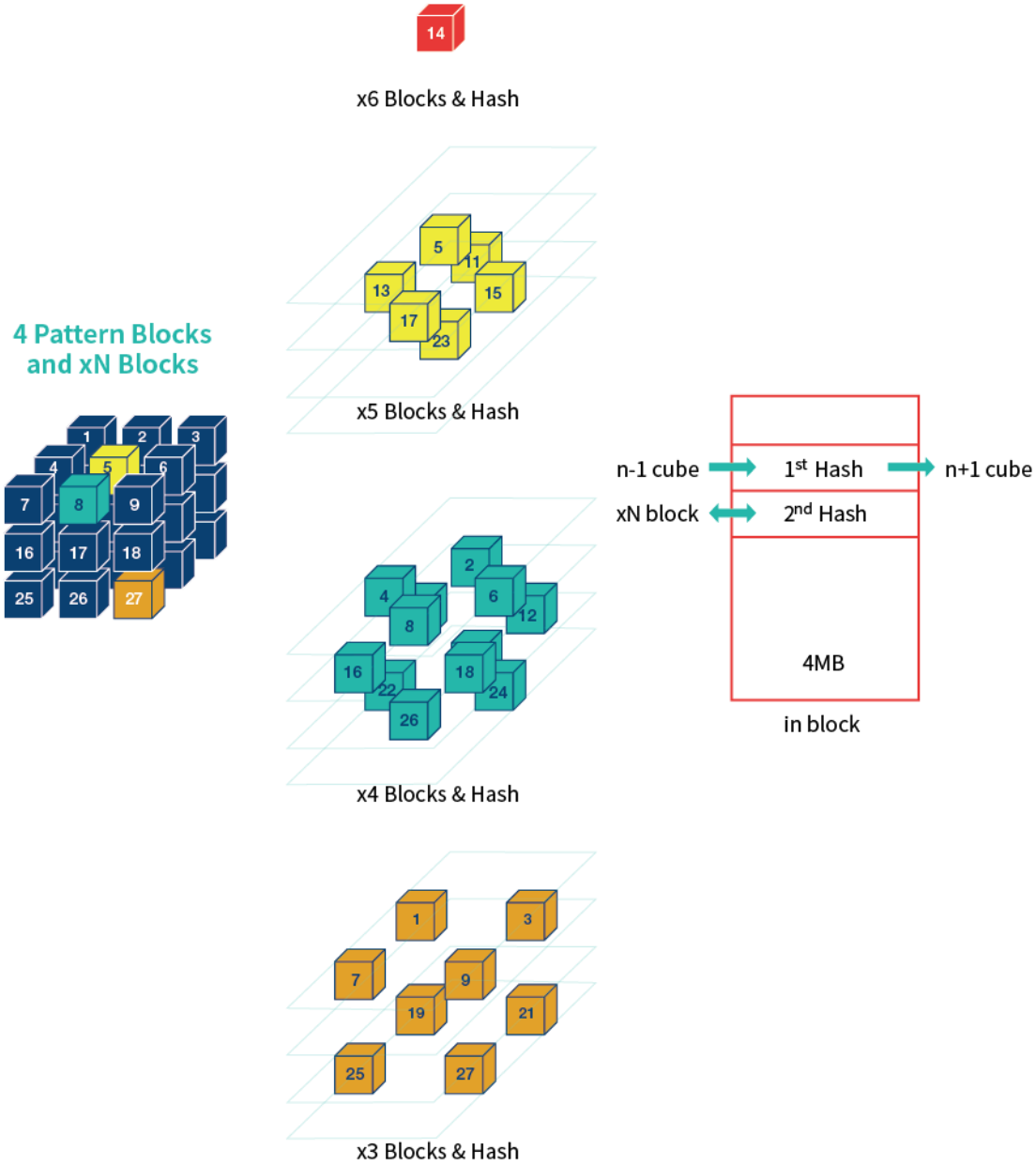
In order to solve the problem of speed reduction and scalability due to the existing serial connection structure, a cube chain, in which data blocks are created in a parallel structure, twenty-four data blocks are created concurrently in the transaction pool and are loaded into the cube, allowing fast and secure processing. It is designed to manage the parallel processing of a large amount of data blocks through the technique of cubing and to realize fast access between blocks by using double hash functions and pattern block structures.

When blocks are combined into one cube, four hash function are used to increase security. The hash function used are SHA256, CH-S1, CHF, SHA384. SHA256 and SHA384 are open hash algorithms. The following describes the hash algorithm which were developed independently. CH-S1 (Cube Hash Special Version 1) is an algorithm developed independently that a special block uses to create hash

function when they are created. CHF (Cube Hash Function) is an algorithm developed independently that is used in the process of cubing to create a hash function with the pattern block.

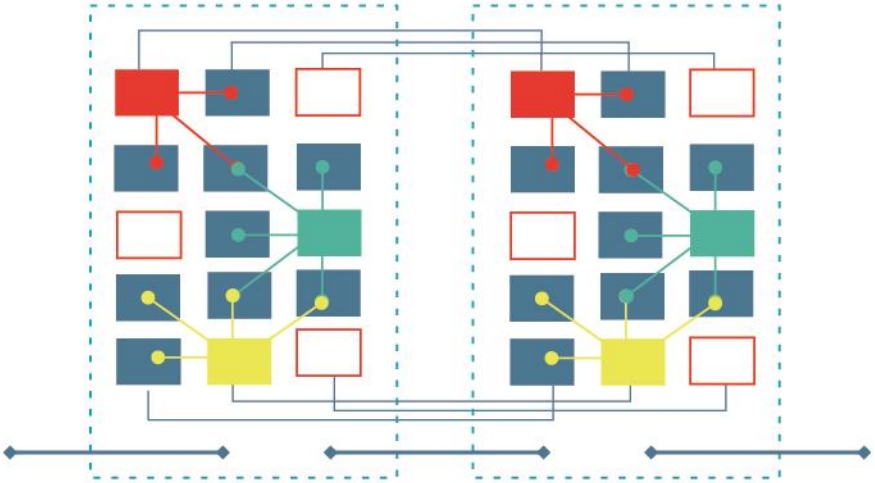
Structural decomposition and description

Cube Chain has a structure that improves velocity by creating and accessing multiple ways of loading the block in a parallel way.



[Figure 3]

When you decompose a cube, there are four different block patterns.



[Figure 4]

Each pattern block is linked with the nearest block of the previous cube and the hash value of the xN block is stored in the 2nd hash. The cube is linked to the cube that had been created immediately before it by storing the hash values of the cube that has been created before in the 1st hash [Figure 2]. It connects the blocks to each other block, and consequently the cubes to each other. The hash value of the block, which is connected by each pattern, is stored in the cube.

2.2 Indexing Block

The indexing block is a block that indexes data for the entire block, enhancing the search function by arranging vast amounts of data clearly. The indexing block is a data block that organizes the cube's height (the block's height of the existing blockchain). Then the electronic wallet is identified in terms of address, which is included throughout the entire transaction. Therefore, indexing blocks can find the corresponding data in the electronic wallet in less time.

For example, within the indexing block, address A: 20c (20: 20th cube, c: 3rd block), 32a, 105h, 201j, 302r Cube block position, address B: 3b, 102v, 201s, 1001q Cube block position and address C: 5c, 34e, 56g, 234k, 456y Cube block position, can be created. As shown, all addresses are arranged in order of the address value, and the corresponding block's height. When a searcher wants to find a specific transaction within the address B, he/she can quickly find the address B is organized due to the

indexing block. The purpose of the indexing block is to help quickly find and easily manage the history of a particular address.

[The existing Blockchain Technique]
Retrieve all data when searching for a specific wallet address transaction history
(When all cubes create 1,000 cubes, 1,000x24=24,000 blocks are searched)
The complexity in terms of time = ***O*(B log2 *T*)**

[Cube Chain Technique]
It only has information about the wallet address, the cube's height, and the block's location. It does not need to scan the entire block with the corresponding data, but can obtain the corresponding data by searching for the wallet address in the indexing block.
The complexity in terms of time = ***O*(log2 *I* + log2 *T*)**
E.g.) Search only the indexing block when searching for a specific wallet address transaction history (1 block + 1 cube)

2.3 Statistics Block

By arranging the statistical values for the entire blocks, the statistics block enables service processing to be much faster. Application services and various APIs also provide rapid logic implementation and a variety of utilizations. A statistics block is a collection of statistical values for the entire blocks to ensure fast data processing. For example, since there are more than 5,000 POS targets within a statistics block, the data for an electronic wallet address with a balance of 5,000 or more, the top 1,000 list of electronic wallets with a high balance, and the list of electronic wallets with more than 100 transfers can be located quickly. Indeed, any statistical data, which is frequently used, can be gathered to quickly generate lists whenever needed.
These statistics are part of a search that requires a great deal of time if there are no statistical values for the entire blocks, but the statistics block allows services to be processed almost immediately.
A collection of frequently used output data, such as the top 1,000 electronic wallets, wallets with high balances and wallets with more than 100 transfers, can be effectively searched. As a result, APIs for applicable application services can be implemented very quickly.

E.g.) A search block to locate the POS target based on cube's height

[The existing blockchain technique]
When the cube's height is 1,000: 1+2+3+ ... +998+999+1,000=500,500x24=12,012,000 blocks
When the cube's height is 10,000: 1+2+3+ ...
+9,998+9,999+10,000=50,005,000x24=1,200,120,000 blocks

[Cube Chain technique]
When the cube's height is 1,000: 1+1+1+ ... +1+1+1=1,000 blocks
When the cube's height is 10,000: 1+1+1+ ... +1+1+1=10,000 blocks

The number of blocks that need to be searched even if there are only 1,000 cubes is 10,000 less using the Cube Chan technique. When considering the process of organizing the list and the process of retrieving the details, a even larger differences will arise. The functions that are considered for transactions in which 1000 QUB, 2000 QUB or more QUB are traded in a single transaction, are the statistics for the balance ranking (1 to 1000), the statistics for the total transaction volume, the total transaction count, and the unauthorized escrow statistics, and all of these statistics are easily searchable, and processed at a much faster rate.

2.4 Escrow Block

Escrow means a service in which a third party, trusted between the seller and the purchaser, intermediates money or goods during a commercial transaction. It is used to ensure the safety of the transaction. The buyer shall assign the payment to a third party. The seller shall confirm the deposit to the third party and then send the goods to the buyer. The buyer shall check the goods sent and notify the third party that the goods have arrived. In any case other than the original agreed upon transaction, the goods may be returned, or the transaction may be cancelled. The third party sends the payment to the seller. The seller will receive the payment or a notification of the termination of the transaction. The third party will receive a certain fee in order to make a profit from the escrow transaction.

Escrow transactions in the Cube Chain becomes unavailable immediately in the wallet of the receiver, even if the transaction is signed for and approved for use. General transactions are recorded in 24 separate data blocks and are recorded in an escrow block during the escrow transaction. Approval encryption can be made and traded in a virtual currency escrow. The approval encryption key allows the sender and receiver to process approvals using the encryption key. At this time, the approved encryption key is automatically generated and sent by the receiver.
As for the authorization technique of the encryption key, only the sender or the receiver can process it for approval. Additionally, only the sender and receiver can accept it. In addition, there is an automatic approval system after a certain period. If key fails to be released the key will be

automatically approved after that period. If automatic approval is granted, the sender will accept it and the escrow status will be maintained until the transaction is allowed by the receiver. The receiver can then request to keep the deal or contract because he/she hasn't cancelled the transaction. In order for the receiver to be allowed to accept the key, and therefore receive payment, the receiver must deliver the approval key via a communication technique, such as e-mail or messenger, to the sender.

In existing escrow transactions, a broker plays the role of a medium for the transaction between the dealers. The escrow block has an escrow function and there is no broker. Although third parties can play an intermediate role as in the existing technique depending on the implementation of the service, there are many special features that escrow introduces through direct inter-party transactions. Escrow blocks could be a revolutionary way to make transactions simple and safe, not only for online shopping malls and open markets, but also for direct transactions between individuals.

The double authorization data system is introduced in the escrow block to store data. The general data is recorded as one of the 24 data blocks, but the escrow data is stored and managed separately. The escrow data is re-written as general data at the time of the double authorization. The term double authorization data system refers to the technique where an encryption key must be additionally issued and approved apart from the electronic signature that is made during transactions by using general blockchain technology. This technique, using the escrow block, the payment is not immediately available in the receiver's wallet, even if the transaction is signed for. This may provide a function to protect transactions between trading parties, other than in the form of current escrow transactions mediated by a third party. In addition, the escrow block can be used by the owner to protect the data with a password, instead of using the data as an open format. Only users who know the password and only those with the encryption key can see the data.

The time required to created and size a regular block and a special block:

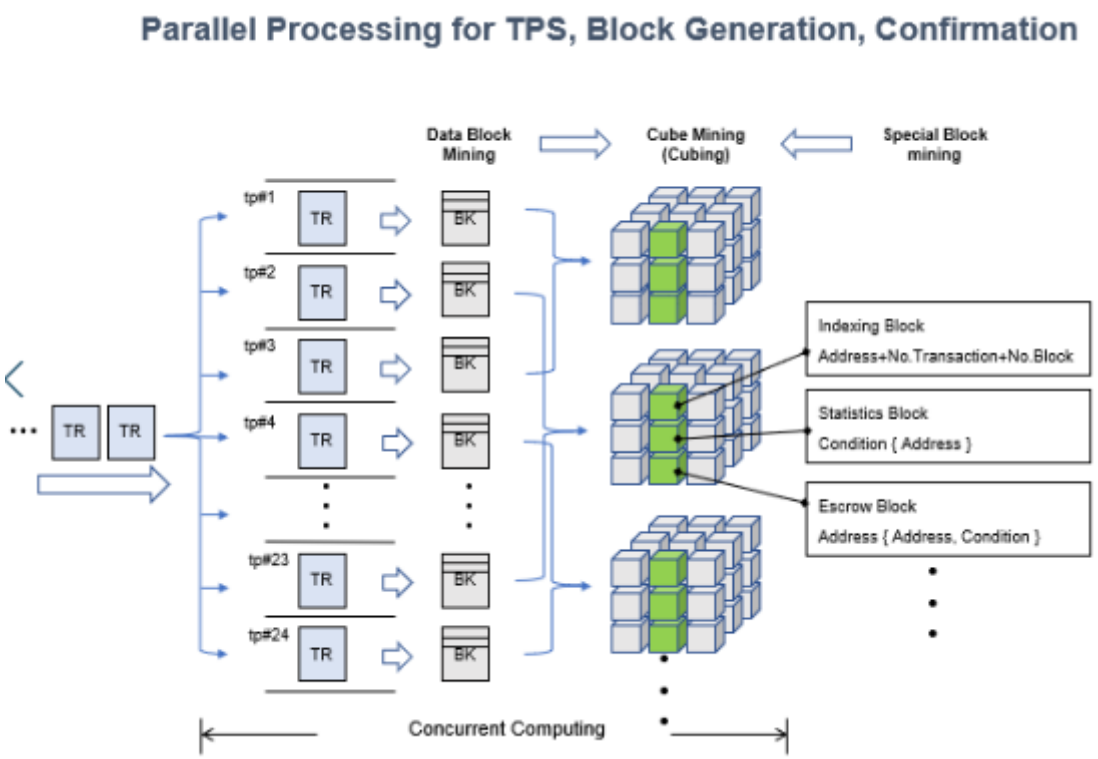
A regular block: One block is 4MB.

A special block: The capacity of the three special blocks is variable, and are created when a regular block is created by cubing.

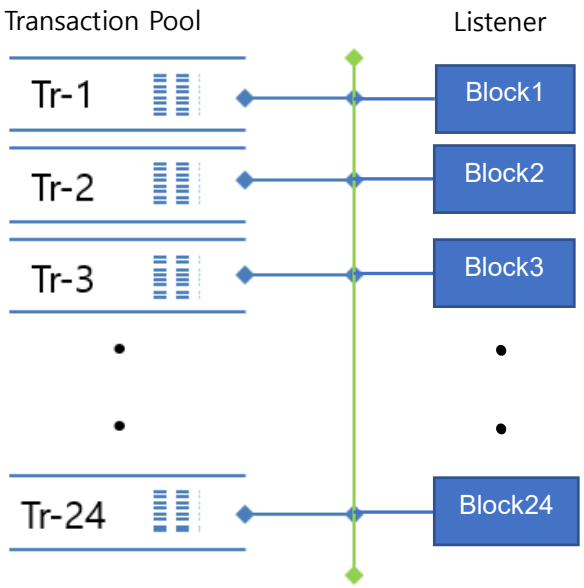
The size of the cube: as the size of a special block is not specified, and is defined as α. 1 cube =24 blocks *4+α, i.e., 1 cube has the size of 96+α MB.

The process from the arrival of the data to the creation of the cube within the transaction pool:

When transaction history or other information (there may be multiple types of input data. However, all encrypted data has the same length and size) arrives in the transaction pool, the data from Tr1 to Tr24 in the transaction pool is allocated sequentially to create a regular block. A special block is created primarily by copying the special block of the previous cube while the previous cube is still being created.



[Figure 5]



[Figure 6]

Each block has a maximum size of 4MB. However, in some cases, it may be less than 4MB. The order of the input data in the transaction pool is defined by the block's order. One transaction is allocated to one block. In this way, parallel processing is conducted. Miners can participate in mining by selecting from the 24 blocks within the allowed resources. Out of the 24 regular blocks, the second and the third block can be selected for mining, and a special block can be selected for mining as well.

2.5 POH (Proof of Hybrid)

Cube Chain adopts the POW+POS Hybrid technique to reduce power waste while inducing participation in the network. The disadvantage is that it takes too long to calculate and pay POS when blending POW and POS. However, with Cube Engine's statistics block function, there is no need to consider the balance because the flaws on calculations are eliminated, and POW and POS ratios are confirmed. The terms of participation in the POS require a balance of at least 5,000 Cube Coins in the wallet and the target who meets the conditions shall be paid in coin compensation according to the balance ratio.

POH is a combination of POW and POS. POW is a protocol (rules and commitment on communication techniques when sending and receiving information between computers) and a program function. POW refers to proof-of-work. POW refers to a system where a person with a large amount hash can find more blocks to acquire coins. It has an economical technique of abandonment by requesting fewer tasks, and may be used to deal with service abuse, such as spam, within the network.

Currently, all coins available for mining are POW, and are popular at the moment. Most of the coins, where the market is the largest and the infrastructure is expanding continuously, utilize the POW technique. (All coins, that issue coins as compensation for solving algorithms, such as Bitcoin, Lightcoin, and Dogecoin, are all now POW coins.)
Because the predominant cryptocurrency is Bitcoin, which is a POW coin, the current mainstream technique is obviously for POW coins. The market size of POW is also much larger than that of POS.
POS is a technique that is designed to address POW's biggest problems: 1) high costs of mining (electricity usage, purchase of equipment), 2) security issues due to the monopoly of the hash.
In terms of POS, with just one PC that is connected to the Internet, everything is available and there is no need to purchase additional equipment, such as better CPUs or GPUs.
Although the way to obtain coins differs in the amount and technique for each coin, the greater the number of coins a user in POS system has, the more coins they will continue to receive (like interest).

In POS, a person who has a large amount of coins takes a large amount out of the coins that are additionally issued. The 'hash' is the main determinate in POW. POS, however, has a standard amount of obtained coins. That is why the POS technique doesn't require a large-scale hash for security. It creates a strong security wall only by having individual coins and an interlocking wallet.

During the launch, large quantities of coins are issued in a short period of time. As a certain amount is steadily issued, and unlike POW which is gradually decreasing, the value of the coin doesn't dramatically fluctuate. It also eliminates the need for large amounts of electricity for a digger to mine, making it easier for more people to get access to and to use the coins.
The increase in the value, however, is not large. There are few reasons for the weakness: 1) large amounts of funds haven't flown in yet (there is less need to hold funds at this point), 2) a person who has more funds can easily monopolize the market, 3) the initial distribution of coins is not even,
Cube Chain started with the POW:POS ratio of 7:3, increasing the proportion of POS over time and eventually maintaining POS only.
At the beginning, it increased POW to ensure a stable network foundation, and used the technique to increase POS, so that power waste could be reduced. There is a disadvantage to blending POW and POS. It takes a long time to calculate and pay POS. However, the statistics block of Cube Chain can dramatically reduce the inefficiency of repeated calculations.

POW is predominant in the beginning because of miners, who are responsible for creating the ecosystem. However, there are a couple of problems, the waste of resources, and inefficiency due to competition. Although it has a high POW at first, Cube Chain makes it possible to adjust the proportion, so that only POS can be used. It distributes the advantages of POW and POS over time, eventually leading to POS gaining an advantage.

3. Encryption Technique

3.1 Creation of Wallet

The most common way to create a wallet is by asymmetric (public key, private key) encryption. Asymmetric encryption has two keys pairs and can be decoded with an additional. One key is a public key, and is used as the wallet address. The other key is a private key, and used as the password for transfers. Cube Chain uses the RSA (Rivest Shamir Adleman) algorithm, which is an asymmetric cryptographic technique for generating the address and password of the wallet.

3.2 Digital Signature

When making a transfer using the wallet, it will be digitally signed using AES256, which is a symmetric cryptographic technique.
The asymmetric cryptographic technique of the RSA Algorithm, which creates the address and the password of the wallet, solves the problem of the transmission of the password, which can't be hacked even when the key is exposed. It, however, has weak point, which is that it is slow. Therefore, it is possible to mitigate the weakness of the RSA by mixing it with AES256, which has some difficulty in exchanging the key, but has a fast velocity for encryption and decryption.

If the size of the data is small, improvements of the data encryption processing technique of creating a digital signature encryption key by using a public key and a private key, which are generated by the RSA will not be efficient. However, the greater the size of the data, the greater improvements of the efficiency.

3.3 Block Hash Function

The hash function is the function that converts data into hash values of fixed length and outputs. The converted data is not used to decode the original data, but is used for verifying the integrity of the data or authenticating a password. The hash value of the ‘n’th block in the blockchain is connected to the hash value of the ‘n-1’th block. In Cube Chain, the hash value of each of the twenty-seven blocks in the corresponding block is created. The hash function used in the data block is SHA-256.

Since the special blocks increases more steadily than the general data blocks, the hash function that is different from the existing hash function, and therefore should be generated by using the CH-S1 function, which was developed independently. The use of existing hash functions can cause a serious decrease in velocity. The CH-S1 hash function greatly improves the velocity of processing by extracting and compressing data.

3.4 Cubing Hash Function

When conducting cubing, the encryption technique should be used with CHF-Algorithm (Cubing Hash Function Algorithm). The twenty-seven blocks in the cube are different from each other depending on the position in the block. It consists of eight blocks located at the corners, six blocks located in the center, twelve blocks surrounding the center, and one central block of the cube, forming the shape of a hexahedron. As the hash function used varies according to the four types of divisions, they are named CH-B3, CH-B4, CH-B5, and CH-B6, respectively.

CH (Cubing Hash) refers to the cubing hash function, and B (Block) refers to the number of blocks that are located within the cube.

The cubing hash function creates another hash value using the hash value of the adjacent block. In this way, the hash value of each of the twenty-seven blocks is obtained.

The advantage of the cubing hash value, as opposed to the block hash value, is that the cubing hash value is based not on the block data, but on the relevant block hash value. The current block and the entire block are verified through the cubing hash value, and the twenty-seven blocks are individually verified by forming the chain relation. The position value within the cube is used to verify each other's block. In this case, the entire value becomes changed even if only one block is different.

3.5 Cube Hash Function

The hash value of the current cube is generated including the total hash value of the 27 blocks obtained from the cube and the hash value of the previous cube. The SHA-384 function is used to create the hash value of the cube.

4. Special Block Generation Process

4.1 Creation of Special Block

In Cube Chain, the special block is not moved by the only the data and is possible to divide and extend the area for the data and the special functions of the data. Three special blocks are set for the cryptocurrency, but the special blocks can also be set separately for other application development. This can be carried out through the Genesis file setting. The special blocks are available for setting when installing the core. It is designed to be easily applied to various fields. In Cube Chain, the special block, which is defined in various ways, has been prepared, and will be added in the future.

4.2 Types of Special Blocks

There are indexing blocks, statistics blocks, escrow blocks, format blocks, and edit blocks, which are all considered to be special blocks. Three of these blocks (index blocks, statistics blocks, escrow blocks) have already been described above.

Format Block

A format block is used when the data format to be recorded on the data block needs to be flexible or must be changed. If the formatting information is changed, a format block will automatically validate the data, preventing invalid data from being included, and thus prevent users or programs from making errors. It only keeps data about the format, but is not used for the general data that users can access.

Edit Block

An edit block is used to modify the existing data. The irreversibility of the blockchain is an advantage and a disadvantage at the same time. It is an essential element for cryptocurrency, but the technology may need to modified for other applications. To do this, an edit block can be set to easily reflect and manage the modifications. The data to be modified is stored in the edit block. When the original data is referred to, the change is reflected in the edit block. As data in the blockchain can be modified and deleted, as well as being a transaction history, it is possible to retrieve, modify, delete, and input data.

However, the format block and the edit block are intended for organizations or companies wishing to introduce a private blockchain. Two of the 24 blocks are converted into special blocks, thus leaving 22 data blocks. It can be understood that the block data can be modified and the position of the data to be referred to is changed instead of the form of the corrected data within the actual blockchain. In other words, it means a conversion from the existing data to data that can be used by a service or an application can be done. The edit and format blocks are not associated with the issue of QUB, but are a special block of options that can be added at the service provider's request.

4.3 The Process for Generation

A special block is data that is reprocessed based on the data block or data to be reflected. The three special blocks are adopted as mandatory special blocks. In order for the special block to be created, there must be a previous data block. Thus, the first cube is created with empty data.

Special blocks are then created from the second cube. The creation of the special block starts at the time the formation of the previous cube is completed. The data blocks to be included in the current cube are included at the time when the creation is completed, and the cubing is subsequently carried out. This process is to prevent the delay caused by the creation of the special blocks in advance. The special block is reflected by adding the contents extracted from the special block data of the previous cube and the contents of the previous data block.

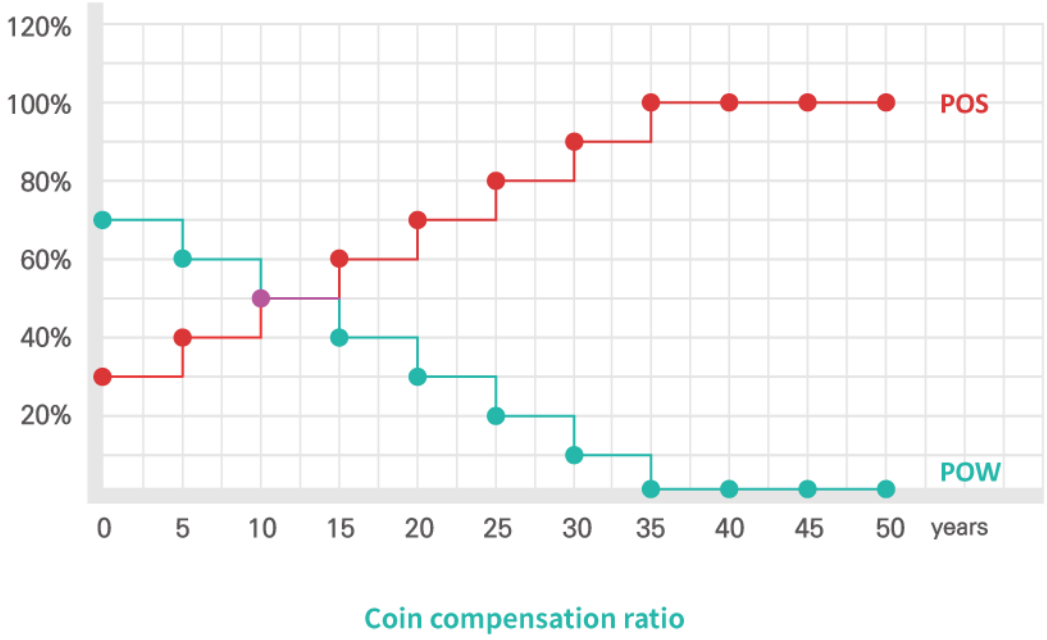
In other words, the special block of the ‘n’th cube contains data up to the data of the ‘(n-1)’th cube. Upon the completion of the ‘(n-1)’th cube, the special block containing the data of the ‘(n-2)’th cube is combined with the ‘(n-1)’th data. When the ‘n’th cubing is formed, it creates an organic relation with the data block. Although the special block is created during the period of chaining the cube, the functional element is expanded, so there is no delay. In addition, the hash value can be obtained at a very high velocity compared to the amount of data by using the CH-S1 function developed by the special block.

5. Agreement Technique

5.1 POH (Proof of Hybrid)

The standard mining technique of Cube Chain is to compensate the coins to the nodes participating in the proof of work. However, in order to solve the problem of increasing the levels of difficulty due to the excessive waste of network resources and excessive competition by caused POW, Cube Chain adopted the POH (Proof of POW + POS hybrid) technique.

The POH technique of Cube Chain gradually increases the POS ratio while progressing POW and POS at the same time after 40 years. It aims to prevent the industrialisation of mining due to POW and to prevent the waste of network resources.



[chart 1]

POW mining can be done in three ways and it can be participated in by selecting each item: the creation of the data block, the creation of the special block, and cubing.

5.2 Compensation Type of POW

The nodes participating in the proof-of-work are given of compensation that is calculated after the creation of each cube.

In the case of participating in the duplication of work, compensation will be given after calculation and pay will be made for each item.

- When the data block is created, the random value added to the hash value is to be compensated for by conducting the calculation. In this case, each of twenty-four data blocks are reimbursed separately and duplicate payments shall be made for duplicate participation.
- When creating the special block, they are compensated by conducting the calculation required to verify the hash value.
- In the process of cubing, by conducting the calculation that verifies the encryption function used for the cubing, they would be compensated.
- It consists of twenty-four general blocks, three special blocks, and one cube. This will be compensated respectively, and duplicate payments shall be made for duplicate participation.

5.3 Data Block Mining Process

- Check the timestamp of the block and the level of difficulty of the node.
- Check that the timestamp of the block is valid as compared to the timestamp of the previous block.
- Create a list of the data or transactions contained in the block.
- Check the Merkle trees of the block header to verify its validity.
- Connect the hash value of the block in the previous cube and create the first hash value.
- Create the second hash value using the pattern block of the previous cube.
- Create the block and spread the block data to the node.

5.4 Special Block Mining Process

The special block mining is a mining technique that only Cube Chain has.

- Check the timestamp of the special block and check the header of the corresponding special block.
- Extract the data to be added to the special block at the data block.
- Calculate the number of data items by the subtotal and the total.
- Create the Merkle trees for this operation and check its validity
- Link the hash value of the block in the previous cube and create the first hash value.
- Create the second hash value using the pattern block of the previous cube.
- Put the data to be added on the previous special block.
- Create the block and spread the block data to the node.

5.5 Cubing Mining Process

The mining of the cubing is conducted as an operation for data structuring in a unique way.

The process of mining for the cubing is as follows.

- Check the timestamp of the previous cube and check the hash value of the twenty-seven blocks.
- Make sure that the timestamp of the cube has a valid time as compared to the timestamp of the previous cube.
- Check the validity of the twenty-seven blocks' hash values.
- Check the validity of the twenty-seven pattern blocks' hash values
- Create a cube hash value using the previous cube hash value and 27 block hash values.
- Create the cube and spread it to the node.

5.6 Diversification of Mining

Cube Chain not only has a wide variety of mining techniques, but also has different efficiencies and the levels of difficulty depending on the technique. POW has been used for the purpose of facilitating network construction in the early stage of Cube Chain, thus broadening the range of participation, so that various participants can participate. This can be done with the mining program and the participating amount of participation and mining blocks should be determined. A chip or a hardware device which decodes the functions used for cubing is to be developed to increase the operational efficiency. This will actualize high efficiency low cost mining and overcome the inefficiency of investing in mining equipment during the period of infinite competition.

5.7 POS Compensation Method

POH is a unique participation technique of Cube Chain that combines the POW mining technique and the POS compensation technique. In Cube Chain, regardless of the participation in the nodes, participation is possible with Cube Chain wallet. Compensation is paid to the holders of more than 5,000 Cube Chain (QUB) based on the previous block, in proportion to the quantity of the cube. However, the amount of Cube Chain (QUB) participating in POS will not be available for transfer. When transferring, only the amount of Cube Chain (QUB) which are not participating in POS will be available for the transfer. The payment can be made at the starting point, when the current block is created, and the amount of payment is determined by calculating the ratio of the amount held as compared to the total amount. In the statistics block of Cube Chain, since the number of POS holders are stored on each block, the compensation amount can be calculated quickly and transferred to each wallet address accordingly.

6. Wallet Service

Cube Chain aims to be a high-availability and convenient blockchain service. To this end, we provide standard services to maximize the utilization of Cube Chain and to provide an environment that can focus on the development of applications and services.

6.1 Cube Chain Wallet Service

The Cube Chain wallet supports services, such as transfers and history management, by using Cube Chain. The Cube Chain Wallet offers a number of distinctive wallet services in addition to basic transfers and transaction history services. As a new financial service that leads to the Fourth Industrial Revolution, it will show the unique identity of the Cube Chain wallet by adding the services that are highly usable and convenient.

Domain service of wallet address

The wallet domain service is a service to match the wallet address, which is difficult to remember, with a specific wallet name that is easy for users to memorize. As with connecting a specific IP address to a specific domain address, it connects a specific wallet address to a user-specified wallet domain address. The wallet domain can use mobile numbers or e-mail addresses, for example. that are used by individuals. The person, who will be making a transfer, will be able to easily remember and enter the wallet domain address. Cube Chain produces address in the type of CWxhQRgBrqZUbj6fj1ftprurb2U9yAFMhu. A simple string, such as Abc.com (case insensitive), can randomly selected by the user and it will replace the complicated wallet address, and it can be used in the Cube Chain wallet.

Wallet grouping service

A grouping service that bundles multiple wallets into a single wallet is a type of service that exposes only the address of the connected wallets without revealing the main wallet address. Users can manage multiple wallet addresses in one wallet, and multiple wallets can be opened or divided according to their purpose. Grouping services can be used to conveniently and easily manage the direct debit service connected to the wallet address.

Direct debit service

Direct debit service is a service that periodically transfers coins to a specific wallet address according to the terms and conditions of the transfer set by the user (receiver, wallet address to be deposited, amount and period). When using the direct debit service, the user can withdraw from their wallet on a designated date without having to notify the recipient. Then it is possible to send a deposit to the recipient and be notified of the details thereof.

Wallet messaging service

This is a function to deliver a confirmation message or a message about a service request to a user of the wallet. This can be used for a few purposes, such as messages upon the completion of transfers or a request to return a wrong transaction. The message is used for notification services within the application.

6.2 Other services

The base service with Cube Chain is a service distributed after building the infrastructure of the base service platform, so that the Cube Chain technology, based on blockchain can be used as a business model for various fields. The purpose of this is to provide a cornerstone for the development of a second Cube Chain application program, which can be used to develop an environment for a company or an individual to make a Cube Chain ecosystem. The base service with Cube Chain will be developed into a completed form that can be applied directly to the business model, and it will be distributed as a template application separately.

Verification service for Cube Chain personal information

It is a personal verification service that can universally be used to store personal emails, mobile numbers, pin numbers, etc. on Cube Chain. The user can provide his/her personal information to the web or application, and that information will be stored on Cube Chain and be released only when the user is authenticated based on the protected data. This provides safely to the user who wants to provide personal information without that information being exposed to a third party.

Cube Chain messaging service

Messaging service based on Cube Chain is differentiated from the traditional messaging service as they are P2P. The messaging data sent and received is transferred to Cube Chain and then stored. As the messaging data is stored in a subordinate order, users can use the service without any delay in data transmission. The distributed data stored on Cube Chain can be converted into a message that is released only to the authenticator. The privacy protection feature is a protective wall that is not exposed or that can be hacked by a third party, allowing users to use a safe chat service. It is also possible to increase the usability by opening the chat room, setting up a participant list, and communicating through API.

Cube Chain file storage service

Cube Chain file storage services allow the user to distribute specific files by using Cube Chain, so that a specific file can be used for public purposes or registered as an authorized file. The service of registering a document file or an image file allows the user to safely store important files.

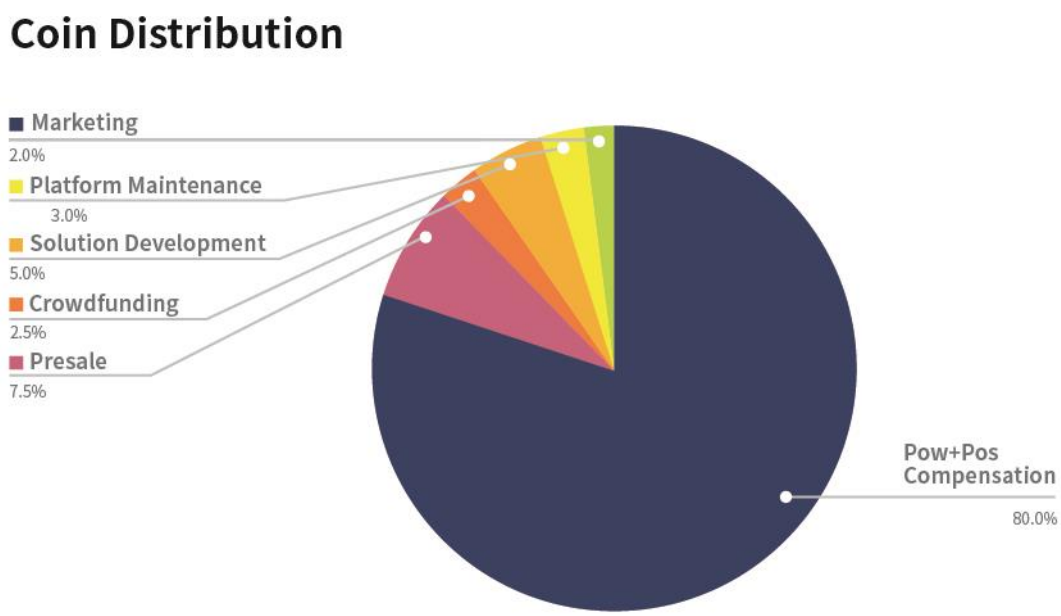
It can also increase the usability of the user's files through services that interlock with template apps or applications.

Cube Chain database service

The database service of Cube Chain is a service for using blockchain data in an efficient way, like in a database. It provides the advantage of structuring and managing data by using the edit blocks and format blocks of Cube Chain. It provides an API to store, modify, and delete data through the standard SQL statements. In addition, it has a feature to interlock the data of Cube Chain with relational DBs by sending data every time a cube is created.

7. Cube Chain Issue Quantity

7.1 Cube Chain Distribution



[chart 2]

7.2 POH Ratio

Cube Chain issue a total of 12 billion coins over 50 years, and the ratio of POW to POS is adjusted over 5-year intervals.

Division	The amount of Cube Chain that has been compensated for 5 years	POW : POS ratio	The amount of the compensated POW	The amount of the compensated POS
~5 years	960,008,400	7:3	672,005,880	288,002,520
5~10 years	960,008,400	6:4	576,005,040	384,003,360
10~15 years	960,008,400	5:5	480,004,200	480,004,200
15~20 years	960,008,400	4:6	384,003,360	576,005,040
20~25 years	960,008,400	3:7	288,002,520	672,005,880
25~30 years	960,008,400	2:8	192,001,680	768,006,720
30~35 years	960,008,400	1:9	96,000,840	864,007,560
35~40 years	960,008,400	0:10	-	960,008,400
40~45 years	960,008,400	0:10	-	960,008,400
45~50 years	960,008,400	0:10	-	960,008,400

[chart 3]

8. Technology Utilization

8.1 RPC Server

The node participating in Cube Chain is available as the RPC server. It can run functions remotely when being used as an RPC server. Therefore, it can control the nodes remotely using Cube Chain. In the nodes of the Cube Chain network, the RPC server can be used to refer to the data of Cube Chain or control the node through a PC or server that doesn't directly participate in Cube Chain. It is also possible to set the limit to the remote sites or to set the range of the functions, so that remote control is available.

8.2 API

By creating and providing API with the Cube Chain RPC server, node management is easy at remote locations. Both the delivery and response of the RPC server's API use the json format. The detailed API document will be opened separately, after the time of processing time of Cube Chain. The API commands and simple examples are as follows:

rpc_ver: get the current version's information of the RPC server.

curl -X POST --data '{"callno":100,"com":"rpc_ver","vars":{},rmsg:"서버 버전 확인요청"}'

network_info: obtain information about the type of network participation, the participating node, and activation state of the server.

curl -X POST --data '{"callno":100,"com":"network_info","vars":{},rmsg:" a request to confirm the network information"}'

p2p_info: get the relevant information on p2p.

curl -X POST --data '{"callno":100,"com":"p2p_info","vars":{},rmsg:"peer to peer info"}'

cube_pow : possible to obtain information on whether to participate in POW.

curl -X POST --data '{"callno":100,"com":"cube_pow","vars":{},rmsg:"confirm the status of POW "}'

cube_pos : possible to get information about the POS of the delivered wallet address.

curl -X POST --data '{"callno":100,"com":"cube_pos", "vars":{"address":"Q9eeb85d32cf465507dd71d503d8a85d32s"},rmsg:" confirm the status of POS"}'

cube_height : get the height of the current chain, in other words, the number of cubes to the present.

curl -X POST --data '{"callno":100,"com":"cube_height","vars":{},rmsg:"confirm the number of chains "}'

cube_balance : confirm the balance of the delivered wallet address.

curl -X POST --data '{"callno":100,"com":"cube_balance","vars":{"address":"Q9eeb85d32cf465507dd71d503d8a85d32s"},rmsg:"confirm the balance of the wallet"}'

cube_transaction_count : confirm the number of transactions of the delivered wallet address.

curl -X POST --data '{"callno":100,"com":"cube_transaction_count","vars":{"address":"Q9eeb85d32cf465507dd71d503d8a85d32s"},rmsg:" confirm the number of transactions of the wallet "}'

cube_transaction_list : Extract he transaction hash value, i.e., the transaction ID. It is possible to find transaction history in a specific address or transaction history at a specific

cube’s height.
curl -X POST --data
'{"callno":100,"com":"cube_transaction_list","vars":{"address":"Q9eeb85d32cf465507dd71d503d8a85d32s"},rmsg:"send the transaction history"}'

cube_transaction_detail : send the history of the hash value of the transaction.
curl -X POST --data
'{"callno":100,"com":"cube_transaction_detail","vars":{"tr_hash":"6e8dd67c5d32be8058bb8eb970870f072445675058bb8eb97f"},rmsg:"send the transaction or data"}'

cube_transaction : proceed with the transaction between the delivered wallet addresses.
curl -X POST --data
'{"callno":100,"com":"cube_transaction","vars":{"address_from":"Q9eeb85d32cf465507dd71d503d8a85d32s","address_to":"Qd2be8058bb8eb970870f0723315b60e8dd","amount":1.2,"fee":0.0001},rmsg:" send the transaction or data"}'

cube_transaction_data : upload the specific data on Cube Chain.
curl -X POST --data
'{"callno":100,"com":"cube_transaction","vars":{"address_from":"Q9eeb85d32cf465507dd71d503d8a85d32s","address_to":"Qd2be8058bb8eb970870f0723315b60e8dd","data":{"no":1,"id":"cubechain","chapter":"cubechain_api","book_name":"Cube Chain whitepaper"}},rmsg:"send the general data"}'

9. Conclusion

The blockchain technology is developing to become the base technology that will lead the Fourth Industrial Revolution. It is not long before the cryptocurrency market will become popular due to technology that ensures both free sharing and the safety of data. Cube Chain intends to mitigate the existing blockchain’s flaws and contribute to the development of blockchain technology. Hopefully, Cube Chain will play a leading role in the Fourth Industrial Revolution, while being widely used in various fields.