# CUBE CHAIN

## Technical White Paper

Cube Engine Version 1.0

Last Updated: Feb 06. 2018

# Contents

# The Cube Chain Technical White Paper

Cube Engine Version 1.0

## 1. Summary

### 1) Introduction

A blockchain is a system collecting several data into a block at a fixed time, verifying them through an encrypted hash value of the block, and storing them into a distributed server. Using cryptography, it ensures reliance on data and security through verification and distributed record.

One of the advantages of a blockchain compared to an existing database is that data will be irreversible as they are verified in chronological order using cryptography. On top of that, it secures and maintains data more safely by sharing and storing same data in a peer-to-peer manner. As it has been applied to digital currency technology that has to show its confidence to a variety of users, it has been rooted in a fundamental technology of the encrypted money market today.

Although an implemented blockchain is unique data recording method using encryption and P2P and opened a new horizon of technology, it still has technical limitations. In order for a blockchain to replace the existing database, it has to have same technical functions that a database has such as improvement of speed, ease of use, etc. If a blockchain technology can be developed gradually and replace the existing database, it will become a secure way of recording and managing data.

From that point of view, Cube Chain enables the functional components of a database to be extended through the concept of cubes instead of blocks. For safer use of a public database, it makes use of some advantages of a database based on those of an existing blockchain. The development of Cube Chain secures the source technology of a blockchain and is about to introduce various online services which issue cryptocurrencies and are in need of a public database.

**2) Overview**

### Cube Chain (QUB)

Coin Name: Cube Chain
Total Amount: 12,000,000,000 QUB
Cube Generation Cycle: 180 secs
Transaction Speed: 100 times per second
Algorithm: SHA-256
Consensus: POH (Proof of POW+POS hybrid)
POS Participation Requirement: At least 5,000 QUB in your wallet
Development Start Date: January 2017
List: Cube Chain (QUB) and discussing listing on several exchanges

## 2. Features of Cube Chain

### 1) Cubing

Cubing refers to a technology for making a cube by combines 27 blocks into a cube. The 24 blocks that record the transaction book and three special blocks are combined to create one cube.

The special blocks are basically composed of three blocks but the number of data blocks can be adjusted and the ratio can be adjusted. As the data block is generated, the cubing is performed and the generated cube creates another hash value. Since the hash value of the block and the hash value of the cube are generated due to the cube, a data system which can be doubly verified can be constructed.

### 2) Indexing Block

Indexing block is a block indexing whole data concisely and intensifies its search function. It is a data block that summarizes an E-Wallet of whole transactions by addresses and cube height (block height of existing blockchain. Thus, an indexing block makes it even faster to find specific data from an E-Wallet. Now it is implemented at a high speed when providing a list output history of electronic wallet or API.

**[Method of the existing blockchain]**
In case of searching a specific E-Wallet address transaction history, retrieve all data.
(When creating all 1,000 cubes, one has to search 24,000 blocks: 1,000x24=24,000)

**[Method of Cube Chain]**
In case of searching a specific E-Wallet address transaction history, retrieve only the indexing block (one block).

### 3) Statistics Block

It is a block that organizes statistical values of whole blocks and expedites the system. To find a certain wallet, you have to search whole blocks of E-Wallets, make lists of balance, and you have to look for E-Wallets containing more than 5,000 QUB. However, if the data of the POS is collected in the statistics block, the search process that is to be repeated every time can be efficiently reduced. It will be very efficient to search data if you collect frequently used data such as a list of top 1,000 of E-Wallets or a list of E-Wallets with more than 100 times of transfers. Consequently, the API of the corresponding application service can be implemented at a high speed.

**Blocks for searching POS by cube height**

**[Method of the existing blockchain]**
When cube height is 1,000, 1+2+3+ ... +998+999+1,000=500,500x24=12,012,000 blocks
When cube height is 10,000, 1+2+3+ ... +9,998+9,999+10,000=50,005,000x24=1,200,120,000 blocks

**[Method of Cube Chain]**
When cube height is 1,000, 1+1+1+ ... +1+1+1=1,000 blocks
When cube height is 10,000, 1+1+1+ ... +1+1+1=10,000 blocks

When cube height is 1,000, there exists 10,000 times difference between the method of blockchain and that of Cube Chain. It only refers to the difference in the amount of data that needs to be retrieved. Considering the process of organizing lists and finding corresponding details, there might be an even bigger difference.

### 4) Escrow Block

An Escrow Block records double approvals data. A Double authorization data system is a method that allows transactions to be made only after double authorization is issued to authorized traders to issue an approved encryption key during the approval process when using a common blockchain. General data is recorded as one of 24 data. However, escrow data are kept separately. When double approvals are made, they have recorded general data again. Although transactions are made, an escrow block records double approval of cryptocurrencies which are from E-Wallets and unavailable to use immediately.

In addition to an escrow account whose money is held by the third party, it has also a protection function for transactions between the parties. It is an escrow function based on a blockchain.
Therefore, it can build secure trading system not only for online shopping malls and open markets but also for direct transactions between individuals. The double approvals method can be implemented in many ways such as sender approval method, recipient approval method, both sides approval, automatic approval method after a specific period, and so on. Escrow blocks can be used by the owner to protect data through passwords, which means only users who know the password through encryption can view the data, rather than using the data in an open format.

### 5) POH (Proof of POW+POS hybrid)

Cube Chain adopts POW and POS hybrid method. In the beginning, the ratio of POW to POS is 7:3. As time goes, the ratio of POS increases and finally it will be maintained only by POS. It increases POW in the beginning stage to make the network stable and raises POS gradually to reduce network resources and power waste. In spite of time-consuming disadvantages for payment when POW and POS are used together, the statistics block of Cube Chain will drastically reduce inefficiency to repeatedly calculate each time.

## 3. Encryption Method

### 1) Creating E-Wallet

The most used method for creating E-wallet is the asymmetric cryptography that uses pairs of keys; one is called public key that is used for encryption and the other is called private key that is used for decryption. The public key is used as an address of the E-Wallet and a private key is used as a password. Cube Chain uses RSA algorithm that is an asymmetric cryptography method for creating address of E-Wallet and its password.

### 2) Digital Signature

When a transfer is made from the E-Wallet, the next step is a digital signature using the symmetric cryptography of AES-256. Although the asymmetric cryptography solved the problem of passing password by creating keys in pairs, it has a drawback because it is slow. As a result, Cube Chain uses a digital signature that creates a password by using public and private keys generated by RSA and it makes data encryption much faster. It is inefficient for the small size of data. However, the larger the data size is, the more efficient it will be.

### 3) Block Hash Function

A block hash function is a function that is used to convert data of arbitrary size into data of fixed size. These fixed size data are used for verifying the integrity of data and authenticating the password, not to decrypt the original data. In the blockchain system, the hash value of the N-th block is combined with that of the N-1th block. However, in 27 blocks make their own hash values by using the hash function of SHA-256. The hash function used in the special block is CH-S1 and uses a self-developed function.
If the special function blocks use the existing hash functions, they cannot avoid speed reduction since the size of data will be larger. In this regard, it is necessary to develop a hash function that will drastically reduce the speed of hash processing for extracting and compressing data.

### 4) Cubing Hash Function

In the process of cubing, Cube Chain uses its self-developed algorithm of encryption. Each of the 27 blocks in a cube has a different neighboring block according to its position. Depending on the position of each face hexahedron, 27 blocks can be categorized into 4 divisions: 8 blocks located at the corner, 6 blocks at the center, 12 blocks surrounding the center, and 1 center block of the cube. Each of 4 divisions uses the different hash function such as CH-B3, CH-B4, CH-B5, and CH-B6. The first CH refers to cubing hash function and the following B indicates the number of neighboring blocks from its position in the cube.

A cubing hash function generates another hash value by using the hash function of its neighboring block. This is the way of having hash functions of each of the 27 blocks. The different

feature of cubing hash from block hash function is based on the related hash functions of blocks, not on block data. Using cubing hash, it verifies the current blocks and the previous blocks and each of the 27 blocks makes a chain relationship individually for verification. The value of the position in the cube is used to verify each other's blocks, and even one block is different during verification each other block, the whole value will be totally different.

#### 5) Cube Hash Function

By using hash functions of 27 blocks in a cube, it creates hash functions of whole cubes. It also enables cubing hash function of the current block to be created by including that of whole cubes and previous blocks. The hash SHA-384 is used for creating cubing hash function.

## 4. The Process of Creating Special Blocks

#### 1) The Setting of Special Blocks

In Cube Chain, not only does it deal with data, it also distinguishes the data area from the special functions data and expands them. Although three special blocks are set for the cryptocurrency, special blocks can be set separately for the development of other applications by setting the Genesis file. Special blocks are designed to be used only when setting the core and easily applied to various fields. Furthermore, various functions of special blocks have been prepared and more will be added continuously in the future.

#### 2) Types of Special Blocks

For special blocks, there are Indexing Block, Statistics Block, Escrow Block, Format Block, Edit Block, and so on. As three of these blocks have been already described, let us find out what the others are.

**ΦFormat Block**

A format block is to be used when the data format to be written to the data block needs to be changed with flexibility. If you change the information of determining to format, the format block will automatically validate data, thereby prohibiting the erroneous data from being included and preventing users or program errors.

**⌀Edit Block**

An edit block is used for modifying existing data. The irreversibility of a blockchain is a disadvantage as well as an advantage. For cryptocurrencies, it is an essential element. However, it may be necessary for data modification to be made for other applications. For this matter, you may set up an edit block and use it for reflecting and managing modifications easily.

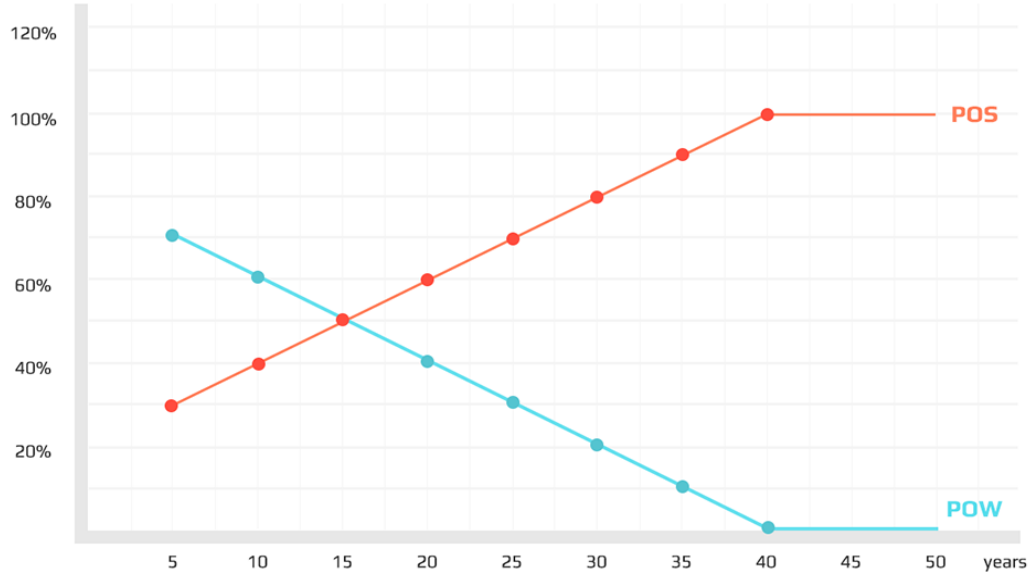
### 3) The Process of Creating Special Blocks

Special blocks are data that reprocessed based on data blocks or data to be reflected. These three special blocks that will be adopted as the essential special blocks are the reprocessed data of the data blocks. A data block has to exist in advance in order for special blocks to be created. For this reason, no special block is created in the first cube. The special blocks are generated from the second cube. The generation of the special blocks is started at the same time that the formation of the previous cube is completed, and the data blocks included in the current cube are included at the time when the generation is completed. The special blocks are cumulatively added by adding the contents extracted from the special blocks of the previous cube and the content of the previous data blocks in advance. That means the special blocks of the N-th cube consists of data up to the N-1th cube. When the N-1th cube is formed completely, the data of the N-1th is combined with the special block of the N-2nd cube. When the Nth cube is created, organic relationship with the data block is made. While the cubes are being chained, the special blocks are generated and the functional element is expanded without delaying time due to this. On top of that, the encryption of the special blocks can be obtained at a high speed by using CH-S1 that is a self-developed hash function.

## 5. Consensus

### 1) POH (Proof of POW+POS hybrid)

The basic mining method of Cube Chain is coin compensation to nodes who are participating in the proof of work. However, in order to solve a problem of excessive power consumption of POW and excessive difficulty due to excessive overheating competition, the POH (Proof of POW+POS hybrid) method combining POS method was adopted. The POH method of the Cube Chain only increases the POS ratio gradually while progressing both of POW and POS at the same time. It aims to prevent industrialization of mining due to POW and to prevent waste of network resources. POW mining can participate in three ways and it can also participate by selecting each item during data block generation, special block generation, and cube work.




< Coin compensation ratio >

### 2) POW's Compensation

The nodes which are participated in the proof-of-work will be paid for a reward by calculation after the creation of each cube. In case of duplication of work, the compensation will be paid in duplicate calculation and each item will be paid in the total amount.

- When a data block is created, it compensates by performing an operation to find an arbitrary value added to the hash value. In this case, compensation is provided separately for each of 24 data blocks, and redundancy is paid in case of overlapping participation.
- When generating special blocks, they will be compensated by performing the operations required for hash value verification.
- Cryptographic functions used for cubing in the process of cubing. In this case, 27 blocks and 4 encryption functions will be compensated for separately.

### 3) Mining Process of Data Blocks

- Check the timestamp of the block and the difficulty level of the node.
- Check whether the timestamp of the block is valid compared with the time stamp of the previous block.
- Make a list of the data or transactions contained in the block.
- Check the validity of the header of the block header.
- Propagate block data to nodes.

### 4) Mining Process of Special Blocks

The mining process of special blocks is as follows:

- Check the timestamp of the special block and header of the special block.
- Extract data to be added to special block in the data block.
- Calculate the number of data by subtotal and grand total.
- Create and verify a validation tree for this calculation.
- Input data to be added to the previous special block.
- Propagate to nodes

### 5) Mining Process of Cubing

The mining of the cube is mined as an operation for data structuring in a unique way called cubing. The mining process of Cubing as follows.

- Check the timestamp of the previous cube and check the hash value of 27 blocks.
- Make sure that the timestamp of the cube is in the valid range as compared to the timestamp of the previous cube.
- Check the validity of 27 block hash values and position values in the cube.
- Proceed to cubing and propagate to nodes.

### 6) Diversification of Mining Method

Cube Chain has various ways of mining as well as the efficiency and difficulty of mining according to the method. The POW is used to smooth the network configuration at the early stage of Cube Chain. In order to increase the efficiency of computation, it is necessary to develop a chip or hardware device that decodes the function used in the cubing process. It is possible to realize high-efficiency mining at low cost and overcome the inefficiency of investing in mining equipment of infinite overheating competition.

## 7) Method of POS's Compensation

POS compensation method
POH is a participation method of Cube Chain that combines the mining method of POW and POS. In Cube Chain, QUB is rewarded to the holders of more than 5,000 QUB balances based on the previous block. At a specific point in time, only those who participate in the Cube Chain node or use POS wallet service among POS persons will be compensated.
Regarding the amount of payment, it shall be paid by calculating the ratio of the quantity retained versus the total quantity. For the time, when the current cube is created, it is paid to the person of the previous cube at the time. Because the Statistics Block stores quantity of POS for every cube, compensation quantity can be quickly calculated and paid to each wallet address.

## 6. Utilization of Cube Chain

### 1) RPC Server

The nodes which are participating in Cube Chain can be used as an RPC server. Since it can execute a function remotely when used as an RPC server, it can control a node at a remote location by using Cube Chain. Using RPC server, it can reference or control node data of Cube Chain through PC or server which does not participate in Cube Chain.

### 2) API

RPC server with API is created and provided so that node management can be done easily from a remote place. Both RPC server API transfer and response use as JSON format basically. The API's usage instructions and simple examples are as follows.

**rpc_ver**: Get the current version information of the RPC server.
curl -X POST --data '{"callno":100,"com":"rpc_ver","vars":{},rmsg:"request server version verification”}’

**Network_info**: Obtain information on the network participation type, participant node and activation status of the server.
curl -X POST --data '{"callno":100,"com":"network_info","vars":{},rmsg:"request network information verification”}’

**p2p_info**: Get information about p2p.
curl -X POST --data '{"callno":100,"com":"p2p_info","vars":{},rmsg:"peer to peer information"}'

**cube_pow**: Get information about POW participation.
curl -X POST --data '{"callno":100,"com":"cube_pow","vars":{},rmsg:"POW check status”}’

**cube_pos**: You can get information about the POS of the delivered wallet address.
curl -X POST --data '{"callno":100,"com":"cube_pos",
"vars":{"address":"Q9eeb85d32cf465507dd71d503d8a85d32s"},rmsg:"POS check status”}’

**cube_height**: Returns the height of the current chain, that is, the number of cubes to the present.
curl -X POST --data '{"callno":100,"com":"cube_height","vars":{},rmsg:"Check the number of chains”}’

**cube_balance**: Check the balance of the delivered wallet address.

curl -X POST –data
'{"callno":100,"com":"cube_balance","vars":{"address":"Q9eeb85d32cf465507dd71d503d8a85d32s"},rmsg:"Check wallet balance”}’

**cube_transaction_count**: Check the number of transactions for the delivered wallet address.
curl -X POST –data
'{"callno":100,"com":"cube_transaction_count","vars":{"address":"Q9eeb85d32cf465507dd71d503d8a85d32s"},rmsg:"Check the number of transactions in wallet”}’

**cube_transaction_list**: Extracts the hash value of the transaction, ie the transaction ID. It can find transaction details of a specific address or transaction details of a specific cube height.
curl -X POST –data
'{"callno":100,"com":"cube_transaction_list","vars":{"address":"Q9eeb85d32cf465507dd71d503d8a85d32s"},rmsg:"Send transaction history”}’

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

**cube_transaction_data**: Put specific data in .
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":" White Paper”}},rmsg:"general data transfer”}’

## 7. Service of Cube Chain

Cube Chain aims to provide a high level of usability and a convenient blockchain service. To this end, we provide basic services to maximize the utilization of Cube Chain and provide an environment that can concentrate on the development of application programs and services.

### 1) Cube Chain Wallet Service

Wallet Service provides services such as transfer and history management using Cube Chain. Wallet Service provides a variety of distinctive wallet services in addition to basic transfer and transaction history inquiry services. As a new financial service, it will show only the identity of Cube Chain wallet service by adding services that are highly usable and add convenience to users when using applications.

#### ① Cube Chain Wallet Address Wallet Domain Service

The Wallet Domain Service is a service that matches wallet addresses that are difficult to remember at one time to specific wallet names that are easy for users to memorize. As if connecting specific IP addresses to a specified domain address, the wallet domain can be a mobile number or an email address that is used by an individual. By using an easy-to-remember address, the user who is to make a transfer or transfer can easily memorize and input the wallet domain address.

#### ② Cube Chain Wallet Grouping Service

A grouping service that bundles multiple wallets into a single purse is a service that exposes only the address of the associated wallet without revealing the address of the main purse. It allows users to manage multiple associated wallet addresses in a single wallet. It is possible to open or classify many wallets according to purpose. It is convenient and easy to manage the direct debit service or connected wallet address by using grouping service.

#### ③ Cube Chain Automatic Transfer Service

The direct debit service is a service that periodically transfers money to a specific purse address according to the transfer condition set by the user (recipient, deposit wallet address, amount, cycle, etc.). With the direct debit service, you can withdraw money from your wallet on a specified date without having to notify the recipient. In addition, it is possible to collectively deposit money in the recipient and notify the details thereof.

#### ④ Cube Chain Wallet Messaging Service

It is a function that can transmit a confirmation message or a message related to a service request to a user who uses a wallet. It can be used as a transfer completion message or a request to return a wrong transaction, and the message can be received by application notification service, SMS and E-mail.

### 2) Cube Chain based service

Cube Chain based service is a service that is deployed after building an underlying service platform to use Cube Chain as a business model in various fields. It forms the development environment to create a chain ecosystem and provides the cornerstone for the development of a more extended secondary application. The base service is developed as a complete form that can be applied directly to the business model and will be distributed separately as a template application.

#### ① The Personal Information Authentication Service of Cube Chain

It is a personal authentication service that can store personal e-mails, phone numbers, pin numbers, etc. Users can provide their personal information stored in Cube Chain on the web or application. The stored personal information is opened only when the user is authenticated based on the protected data so that the stored personal information can be safely interlocked with the user who wants to provide the personal information without being exposed to the third party.

#### ② Messaging Service

Cube Chain messaging service is differentiated from existing messaging services in that P2P services are in progress, and messaging data is sent and stored in Cube Chain. Data stored in a can be transformed into a message that is opened only to the authenticator, with privacy protection applied. Privacy protection is a protective barrier that is not exposed or hacked by a third party, in addition, it is possible to increase the usability by opening chat rooms, setting up participants, and communicating conversation contents through API.

#### ③ Saving Files Service

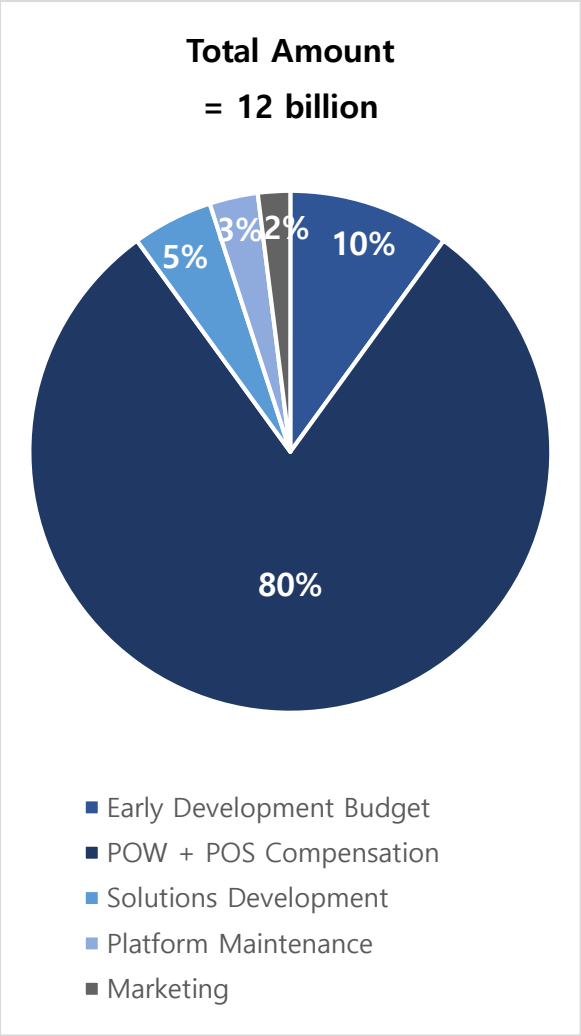
File Storage service allows a user to distribute a specific file by using Cube Chain so that a specific file can be used for public purposes or registered as an authorized file. You can keep important files safe. You can also increase the usability of your files through services that work with template apps or applications.

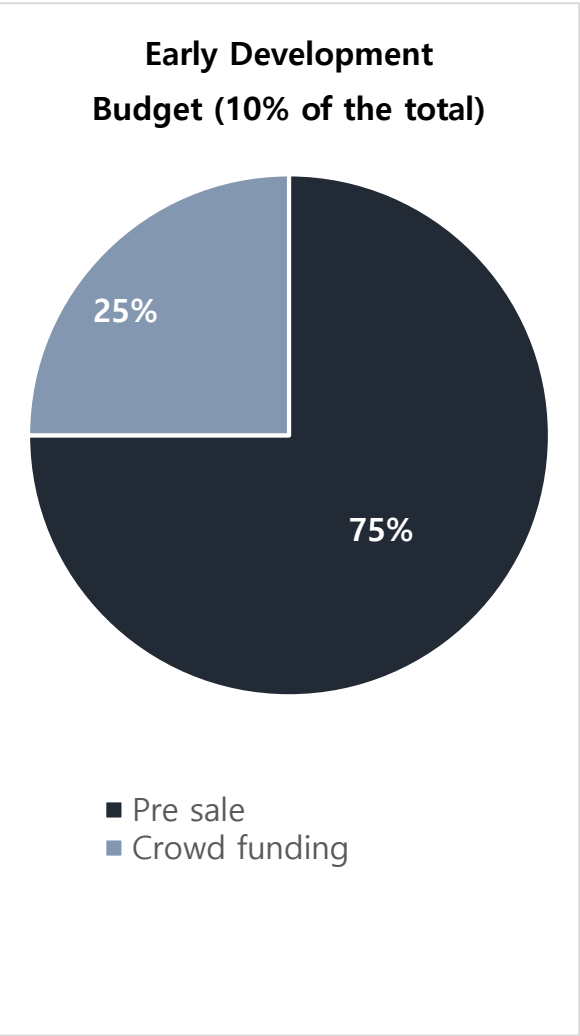
#### ④ Database Service

The database service is a service for using the data of the blockchain as high as the database. It provides the advantage of structuring and managing the data by using the edit block and the normalization block of. It provides API to save, modify and delete data through standard SQL statement. It also provides a function to relate data to the relational database by sending data whenever cube is generated.

## 8. Cube Chain Distribution

### 1) Distribution



**2) POH Ratio**

12 billion QUB will have been issued over 50 years. 80% of the total amount is 9,600,960,000 QUB. We compensate with the consensus “POH” and the ratio of POW to POS is adjusted every five years. A cube is created every three minutes and compensates for 1,096 QUB each time a cube is created.

| Classification | Mining quantity For five years | Created block Quantity for five years | Mining Reward Quantity Per cube | POW : POS rate | POW reward quantity Per cube | POS reward quantity per cube |
|---|---|---|---|---|---|---|
| 5 years | 960,096,000 | 876,000 | 1096 | 7:3 | 767.2 | 328.8 |
| 10 years | 960,096,000 | 876,000 | 1096 | 6:4 | 657.6 | 438.4 |
| 15years | 960,096,000 | 876,000 | 1096 | 5:5 | 548 | 548 |
| 20years | 960,096,000 | 876,000 | 1096 | 4:6 | 438.4 | 657.6 |
| 25 years | 960,096,000 | 876,000 | 1096 | 3:7 | 328.8 | 767.2 |
| 30years | 960,096,000 | 876,000 | 1096 | 2:8 | 219.2 | 876.8 |
| 35 years | 960,096,000 | 876,000 | 1096 | 1:9 | 109.6 | 986.4 |
| 40years | 960,096,000 | 876,000 | 1096 | 0:10 | 0 | 1096 |
| 45 years | 960,096,000 | 876,000 | 1096 | 0:10 | 0 | 1096 |
| 50 years | 960,096,000 | 876,000 | 1096 | 0:10 | 0 | 1096 |

## 9. Conclusion

The blockchain technology is evolving to become the base technology to lead the fourth industrial revolution. It will not be long before it will be popularized as a technology that secures free sharing of data and security at the same time, as well as in the encryption currency market. Cube Chain aims to contribute to the development of the blockchain technology by complementing the shortcomings of the existing blockchain. Cube Chain will play a leading role in the 4th industrial revolution and at the same time be widely used in various fields.