modltoken.io

Whitepaper for MODULE JP ver. 1.0

Index

Disclaimer of Liability

Disclaimer of Liability

This document is a White Paper that describes present and future development, with forward-looking statements that are not deterministic or assertive, and which may be subject to changes and updates. This document is only intended to provide information, and, unless explicitly specified, the products and technologies described in this document are under development. There is no guarantee that this development or other related activities will lead to a successful outcome.

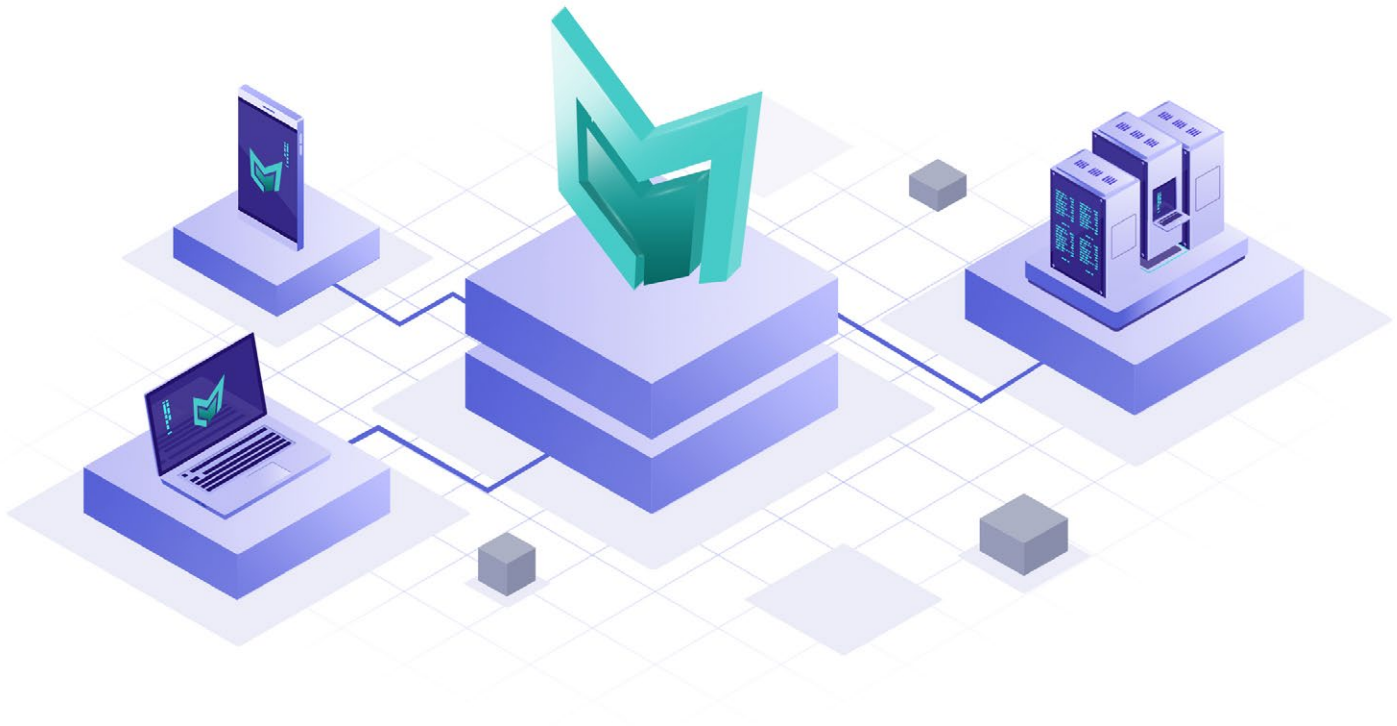
The creators have included their current forecast in this document, which is subject to risk and uncertainties, as it is based on factors such as the public information on possibilities, business strategies, plans, future business objectives, laws, regulations and technologies at the time of publishing. Actual results may differ significantly from the contents explicitly or implicitly implied in this document.

The creators of this document have no obligation, and do not accept any responsibility, to update or change any forward-looking statements based on new information or other subsequent events. In light of the existing uncertainty and potential conflicts of interests, we do not recommend that you rely solely on the future prospects and forecasts included in this material. For individual economic decisions and inquiries concerning taxation, please consult with your legal and tax advisors.

Additionally, the Module Token (Currency Symbol: MODL) does not have the properties of a security. The objective of this White Paper is not to solicit investments, and does not represent a call for investment in securities.

1. Executive summary

MODULE is a blockchain-based platform designed to utilize the free storage of smartphones, PCs, servers, etc. as an asset. Using the MODULE platform, one will be able to participate in mining even from a smartphone. Servers and enterprises can also participate in mining.



Module's consensus (mining) algorithm makes it possible to earn rewards by lending out storage space. As the storage capacity of devices progresses and expands, one can expect the various services offered to expand. In addition to issuing new original coins, users will also be able to develop Dapps (decentralized applications) on the platform.

2. Introduction

Due to their vast potential, cryptocurrencies are currently attracting global attention. There are still problems, however, such as the power consumption of PoW (Proof-of-Work) and centralization of PoS (Proof-of-Stake). Numerous cryptocurrencies are working on improvements on a daily basis. Nevertheless, to date no fundamental solution has been reached, as the improvements tend to remain inside the conventional framework of blockchain.

Miners who possess equipment, obtained by huge investing into it, monopolize profits

As one can obtain the right for approval because of the amount of currency possessed, the liquidity of the currencies is violated, and the gap between rich and poor is growing

Reward
PoW

Capitalism
Centralization

Reward
PoS

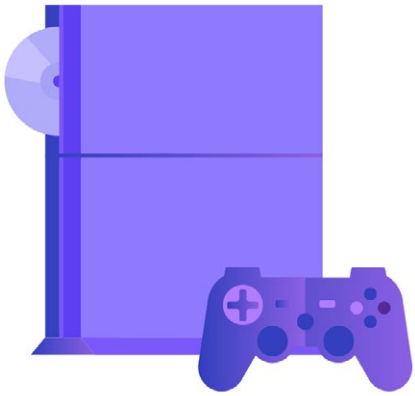
There is a paradox on the cryptocurrency market. Small groups of people with a huge amount of capital possess cryptocurrencies, which runs counter to the original idea of the virtual currencies ushering in an era of decentralization. As a result, blockchain today has become centralized, and may have squandered the opportunity to spearhead financial reform and lost its true value in the process. In this sense MODULE is about to implement true decentralization.

The more cryptocurrency a person possesses, the more influence he/she can exert over the market, thus contributing to inequality and widening the gap between rich and poor. Miners who are able to invest heavily possess the necessary equipment, and monopolize profits.

In this sense MODULE is about to implement true decentralization

2. Introduction

About platform



Platform is a basic part of products and services. For example, home video game consoles or portable game consoles are the platform. Game software which can enjoyed on the consoles is a service.

Game types differ depending on the type of a console. A platform is usually a “basis”, specializing in a certain genre.

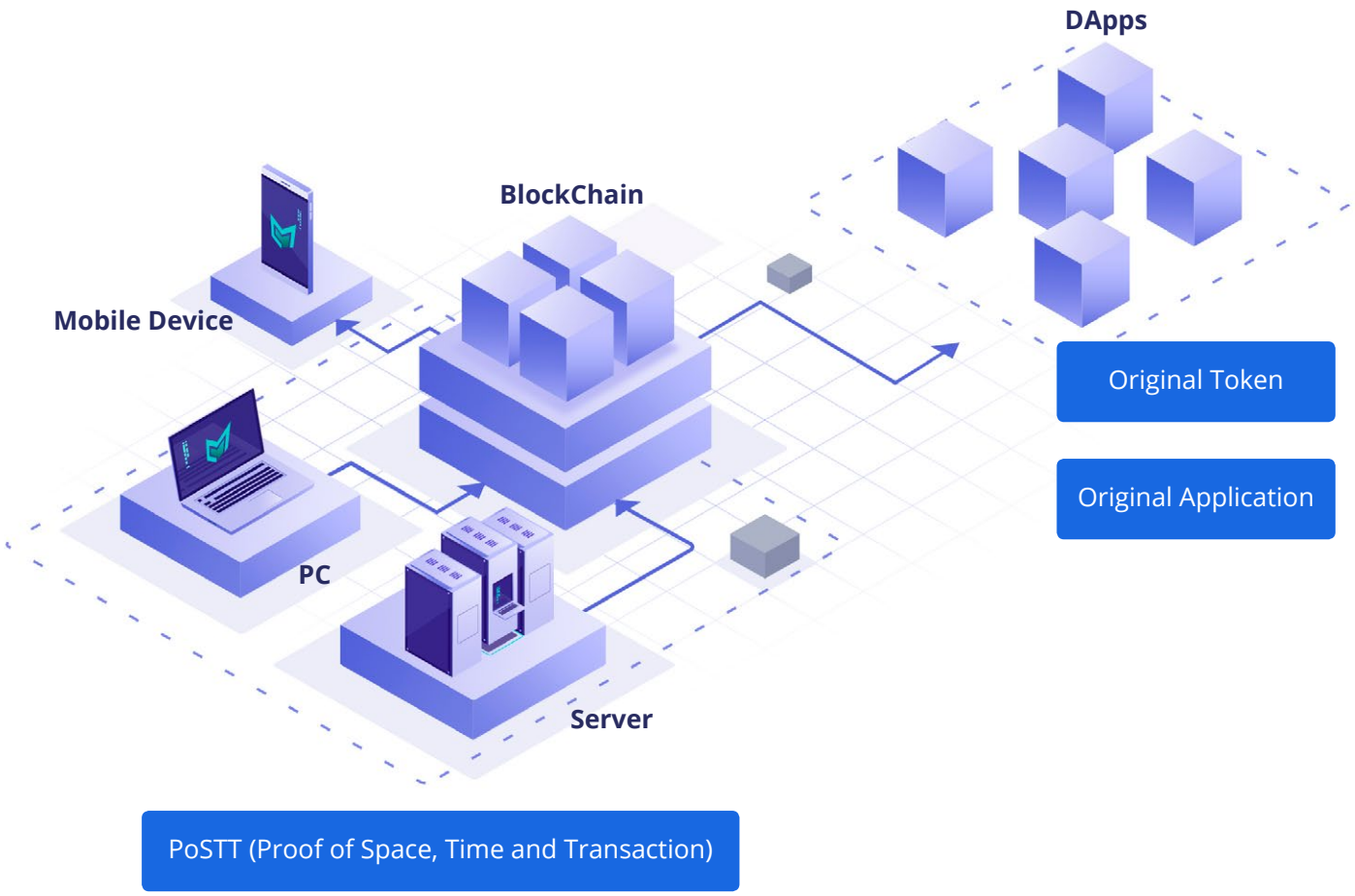
The MODULE platform will combine various parts and will be useful for developing distributed applications.

2. Introduction

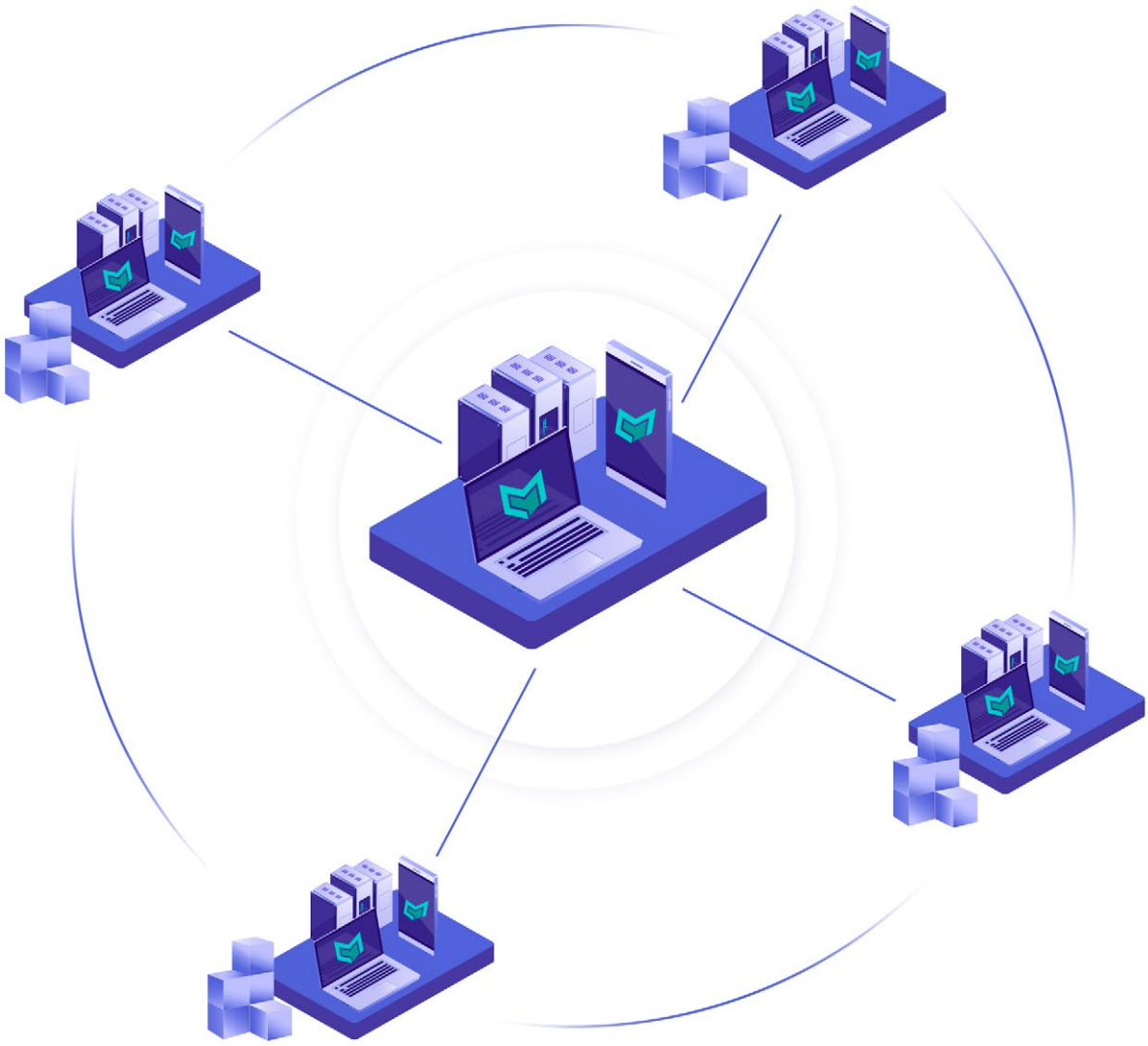
About MODULE

About the MODULE platform

MODULE employs a new transaction approval algorithm. It is a new technology platform that enables everyone to participate in mining, even from a mobile device. In addition to building DApps, users will also have the ability to issue new currencies on the platform.



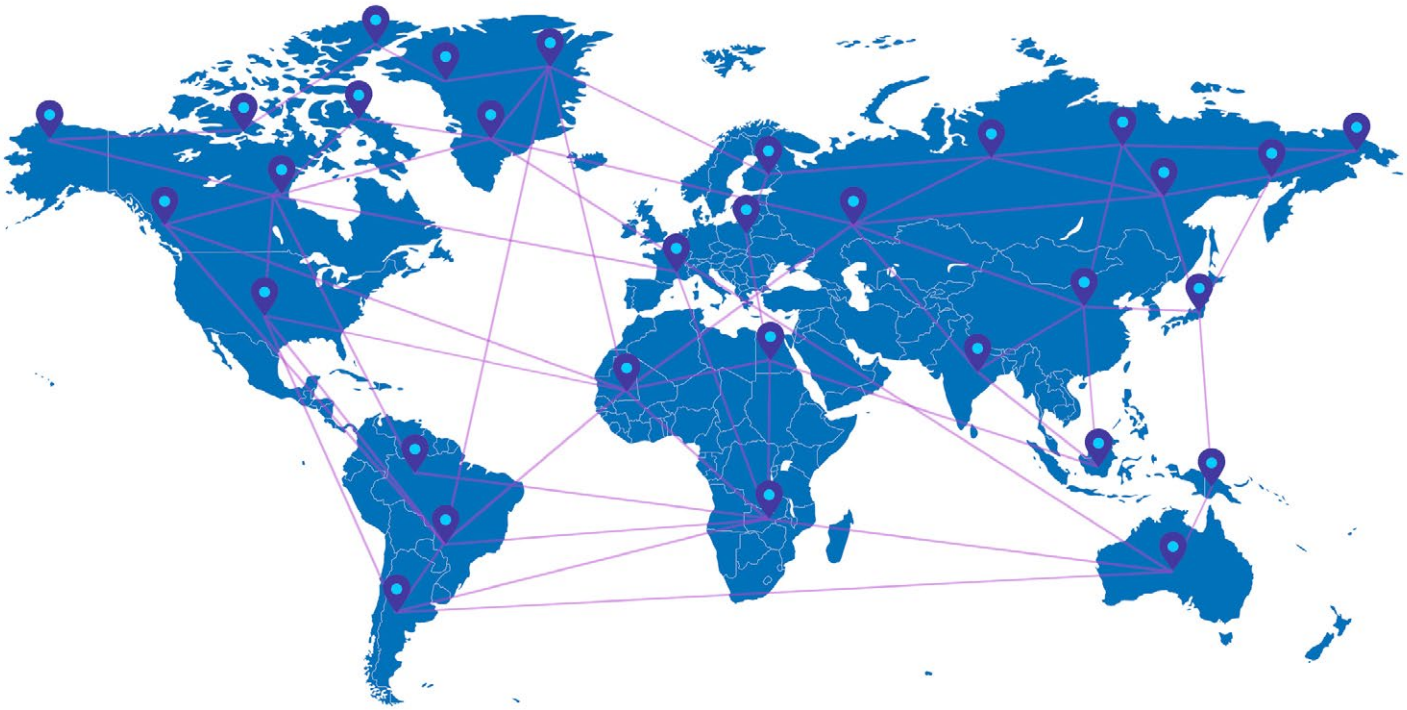
2. Introduction



We focused on mobile devices as a way to solve problems such as the power consumption concerns caused by cryptocurrencies and their centralization. The Module project announces the future of mining with such energy-efficient and easy to use devices such as smartphones and tablets. By releasing the capacity of your device, you will be able to earn rewards, which will vary depending on the capacity of free storage, utilization time, space and transaction type. In other words, lending of storage space will make you eligible for compensation. The platform also has great potential as a platform that can provide other distributed application services.

2. Introduction

The Future According to MODULE



Although the popularity of cryptocurrencies hasrisen, there are still very few chances to use them in real life. Bitcoins can be used at some shops, etc., but the required infrastructure is still under development. We want to bring cryptocurrencies into the mainstream.

The MODULE developers have devised a new algorithm. The team is developing a system under which compensation is determined based on three elements of storage: space-timetransaction. This will enable users to participate in mining from mobile devices such as smartphones.

In our future, not only people living in developed countries will have the opportunity to participate in mining. We hope to have many people holding smartphones in underdeveloped countries acting as miners and receiving rewards. For many people in developed countries, mining that brings in only one dollar a day may be meaningless, but we believe that this can drastically change the life of people in poorer countries.

2. Introduction

About Storage Surplus

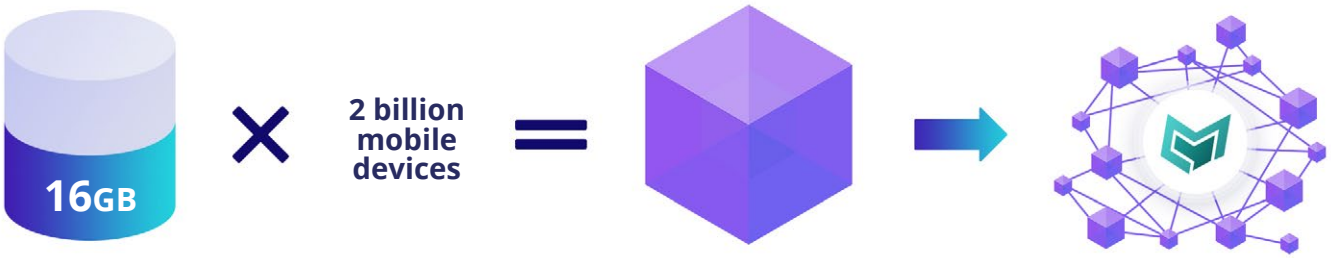
Can you imagine how much storage in the world is not used?

Assumption:

Mobile storage: **32GB on average**

Percentage of storage utilization: **50%**

Total number of mobile devices: **Approximately 2 billion**



Unused (16GB) | **Approximately 32 billion GB** | **Unused resources**

Effective use in the MODULE platform

That means we have vast storage resources on the planet that are being wasted. MODULE is the platform that intends to use these storage resources. We aim to become an environmentally friendly platform by effectively utilizing unused assets.

3. Technology

Overview

The PCSN (P2P Cloud Storage Network), which made client-side encryption possible, enables a user to transmit and share data without having to rely on a third party's storage space. The elimination of central control can alleviate problems such as traditional data errors and power cuts, while significantly increasing security, privacy and data control. Earlier, the P2P network was not suited for building a storage system. With this system we solve the inherent problems by implementing direct payment (Suggested solution) — (Method similar to the response verification system). This will enable data authenticity to be checked on a regular basis, and compensation to be paid for the data stored in PEER. We also propose an address access model and independence in this system, as well as the ability for the nodes to aggregate.

Introduction

Cloud storage is used to provide massive storage space, which plays the same role in data storage and transmission as verified third-party organizations. However, the problem with this system is that it is a TRUST-BASED model. This is not only because client-side encryption is uncommon, but also because up to now clouds have suffered from the loss of personal data and confidential information due to attacks by hackers who were aware of the vulnerability of the server and programs to malware. As many storage servers rely on the same infrastructure, there is the risk that malware could affect the entire system via files.

A distributed storage network has advantages over a cloud-based server. Data security is maintained through client-side encryption, while the reliability of data is maintained through proof of decryption. It is also possible to significantly reduce the impact of server malfunctions and security violations (security risks). The introduction of more advanced devices and the use of a constantly growing number of devices will allow the cost of data storage space to be reduced.

Data on the network will be highly resistant to any unauthorized changes, unauthorized access or data errors. A more detailed description is given below.

Unique mining method “PoSTT”

~ Proof of Space, Time and Transaction

Overview of the PoSTT Proof of Space, Time and Transaction) protocol

The POSTT protocol creates a decentralized storage network with its own coins (or tokens) provided by P2P.

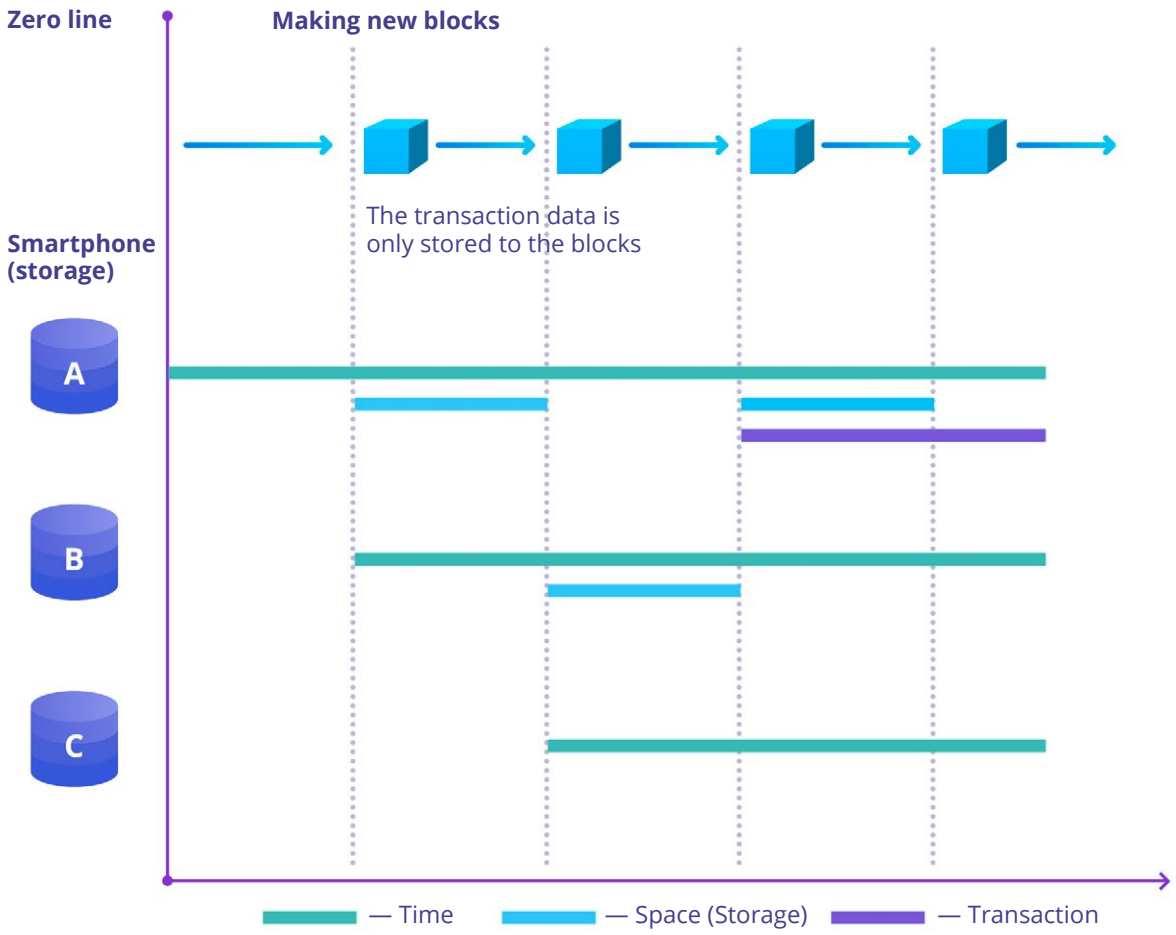
Clients will use the tokens for storing and transmitting data, and miners will mine the coins (tokens) used for data storage, services, etc.

Consensus Algorithm

The POSTT decentralized storage network can perform data storage and data transfer (downloading etc.) functions across two markets. The two markets are the data storage market and the data service market. A client and a miner determine the service price, form an ORDER in the market, and process each ORDER.

This market is developed by POSTT, which includes both POS (Proof of Space) and POTT (Proof of Time and Transaction). Users will be able to store their data safely for any period of time they want.

Finally, miners will support the blockchain by generating new blocks, and the opportunity for miners to earn rewards for exerting influence on the new blocks will be proportional to the storage space, time, and the number of transactions currently provided to the network.



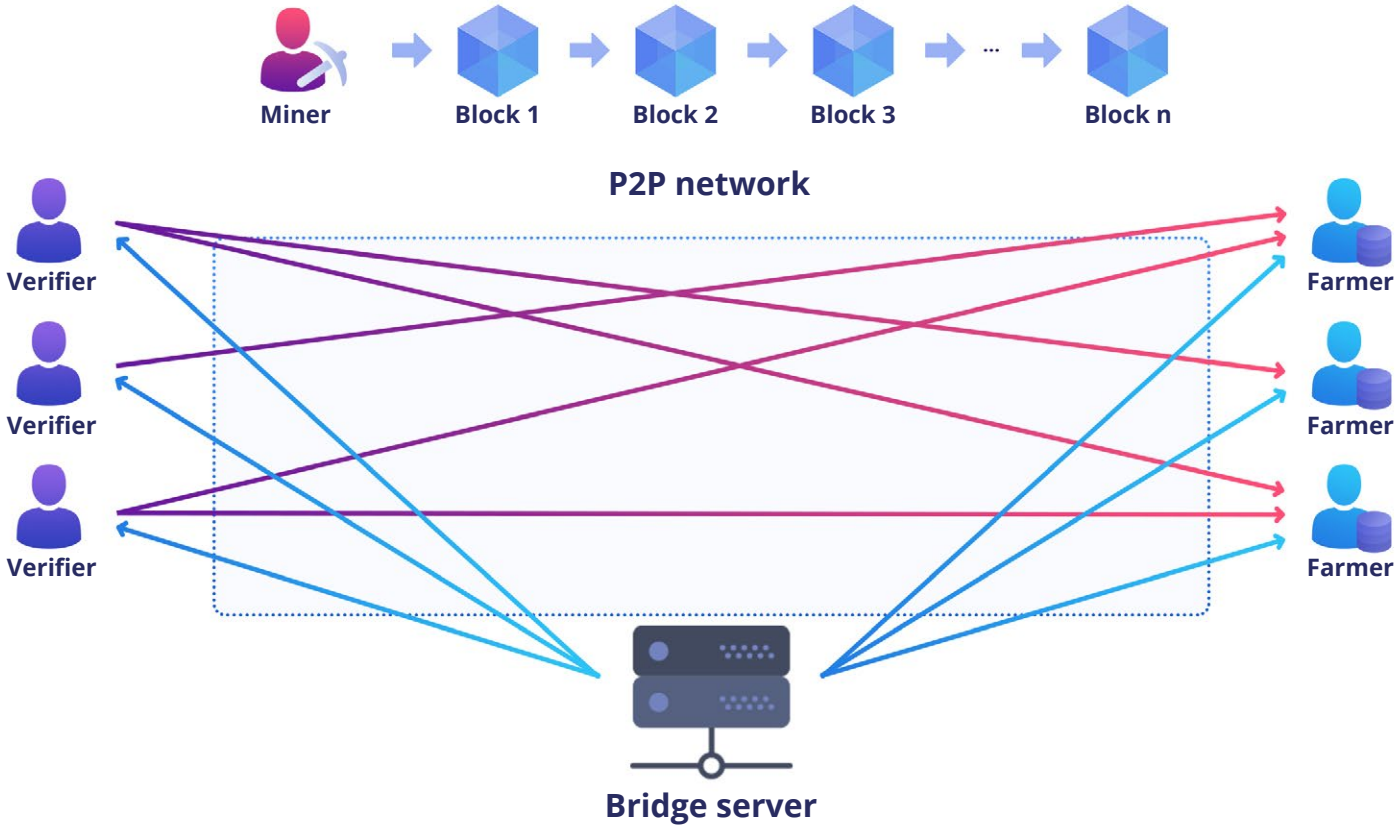
3. Technology

1. About the PoSTT block chain mechanism

The PoSTT blockchain was born from the idea to introduce blockchain technology to existing cloud-based servers. The existing client-server solution is plagued by problems of server management costs and hacker attacks. In a client-server solution, the user's data are stored in the client's server, and data may leak or be destroyed if the server is attacked. However, this data security problem can be resolved by distributing and storing the user's data using the P2P method on blockchain. Besides, data can be stored at a lower cost.

Nodes participating in the PoSTT block chain

- Node that is requesting data storage (Verifier): a node that attempts to divide data and store it in the P2P network
- Node that provides storage capacity (Farmer): a node that provides storage capacity on the P2P network and receives rewards (coins) for data storage
- Node which maintains the blockchain (Miner): a node that verifies the transaction history and smart contract, generates blocks and maintains the blockchain



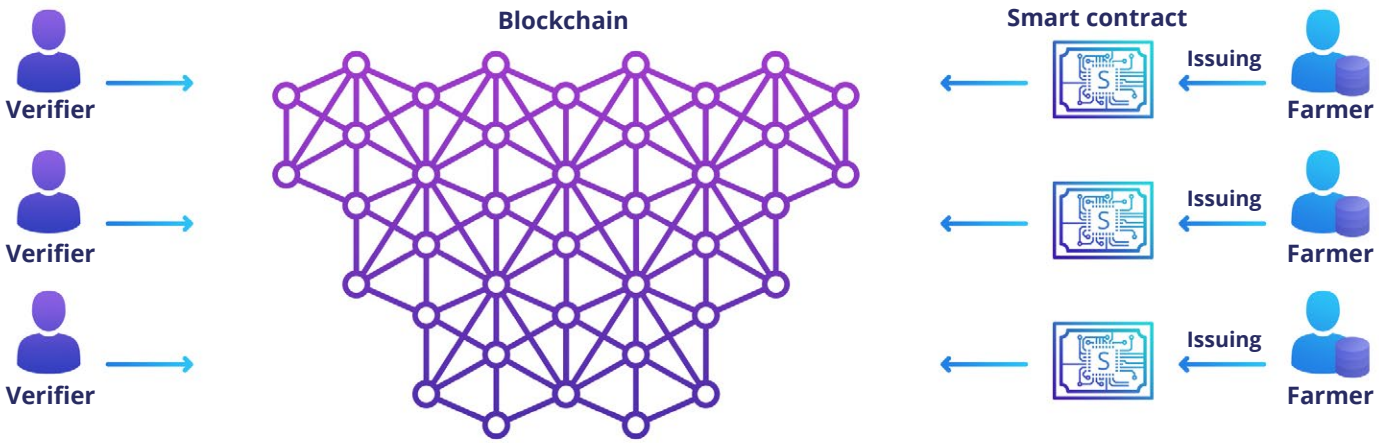
3. Technology

Mechanism of the PoSTT blockchain

1. **The PoSTT blockchain has its own coin.**
   The Verifier will pay the cost of storing the data with this coin, and the Farmer will receive coins as compensation for providing storage capacity to store the data. This means that the PoSTT blockchain has a transaction function associated with the sending and receiving of coins.

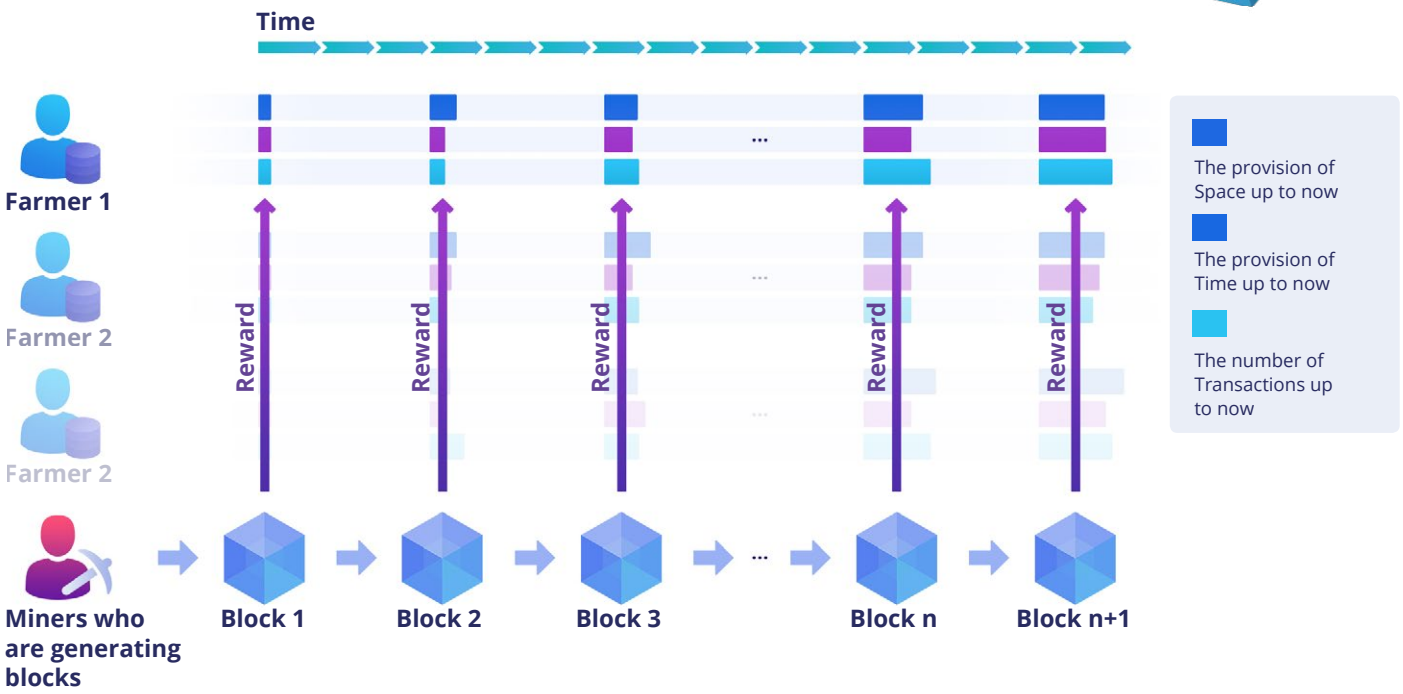
2. The Verifier and the Farmer also conclude a smart contract related to storing each other's data, so that the Verifier and the Farmer can safely perform data processing. In other words, blockchain stores smart contracts related to transactions with coins (transmission/reception) and data management. To do so, the Farmer possess the address of the token for the smart contract. There is also a bridge server which exists separately from blockchain.

The Bridge server monitors the current P2P network and blockchain, and acts as a relayer that chooses which Farmer's network the data from the Verifier should be stored and informs the Verifier of this.



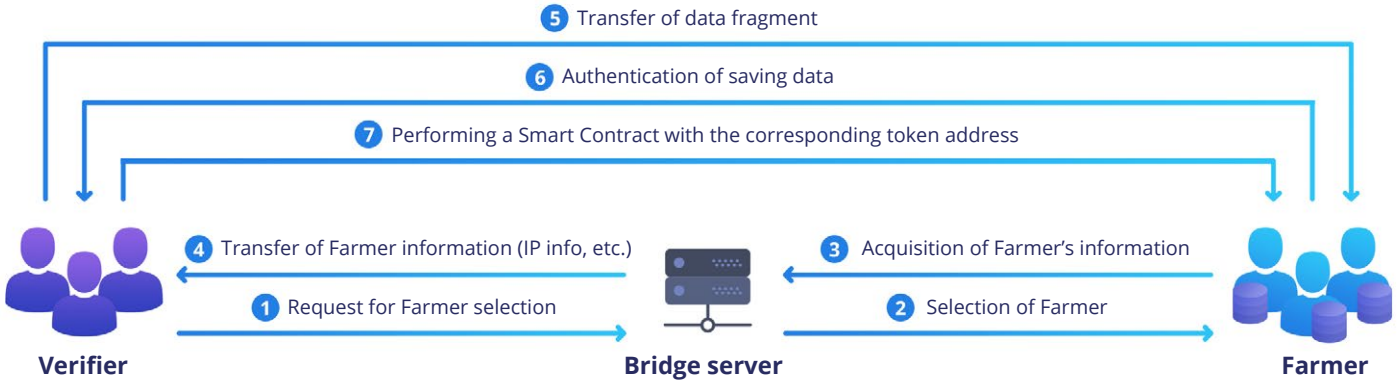
3. **Finally, there is the Miner, who maintains the blockchain.**
   The Miner 1) checks the content of the smart contract related to the transaction of created coins and uploading/downloading the data, and 2) generates the block. The Miner implements the Farmer's calculation logic for the compensation payment and issues coins to the Farmer when the block is created.

3. Technology



4. Bridge server (hereinafter referred to as the Bridge)

The Bridge forms the connection between the Farmer and the Verifier. The Bridge stores only MetaData, not the personal data of the Verifier. The Bridge periodically checks the status of the Farmer and monitors the accuracy and validity of the data stored in the Farmer's network, the status of the data and the payment relationship. By providing API, the Bridge gives other blockchain developers the opportunity to extend various functions of the PoSTT blocks. Using this API, the developer can check the current state of the blockchain state and so on, and develop various programs using the PoSTT blockchain. The Bridge also includes algorithms such as file status, setting the criteria for the selection of a Farmer, and so on. In addition, the Merkle Tree function will establish mutual trust between the Farmer and the Verifier and serve as verification of file accuracy.

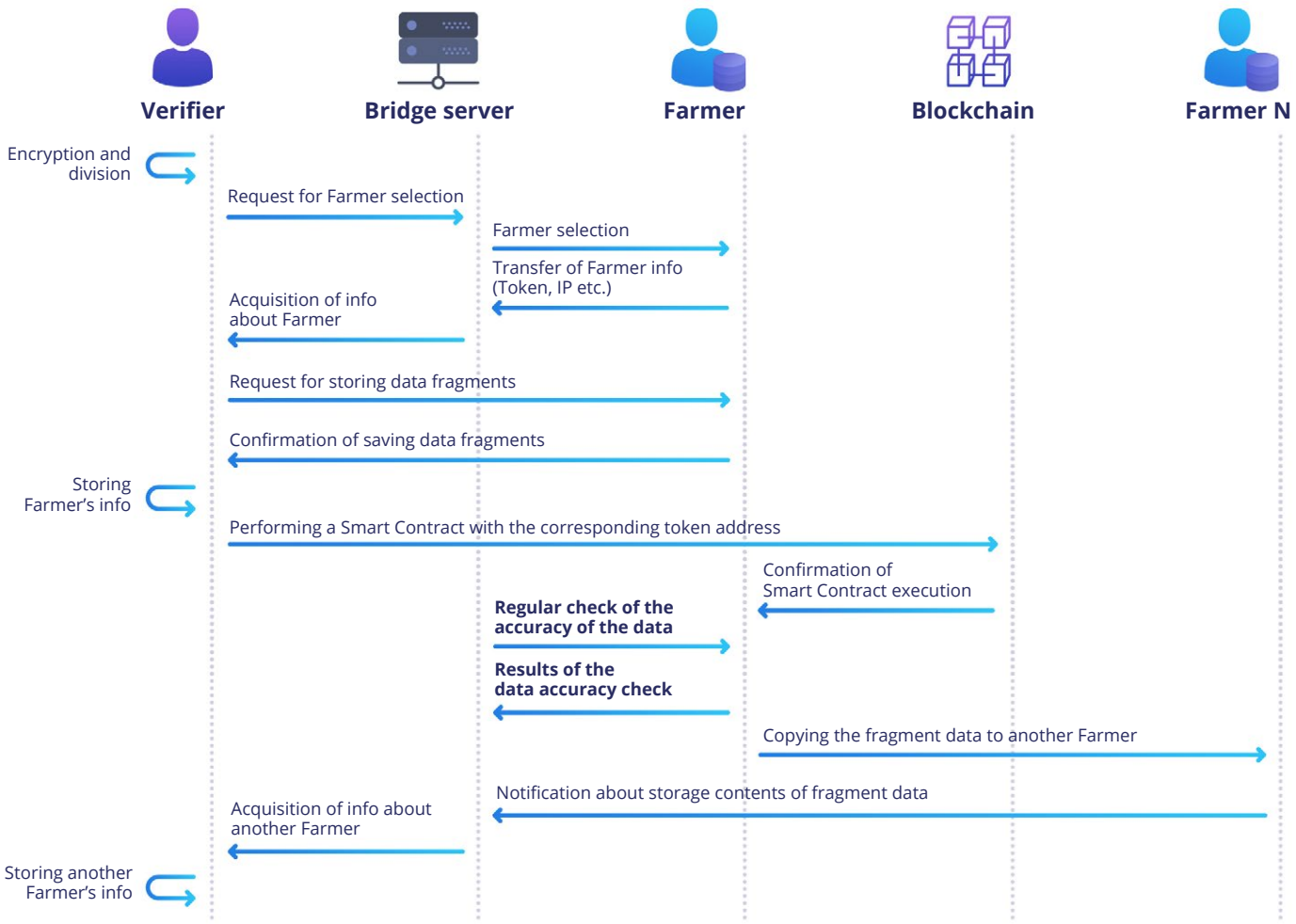


2. Reward system in PoSTT and the process of uploading/ downloading data

The reward system in the PoSTT blockchain is as follows.
In the PoSTT blockchain, the reward is proportional to the size of the data, the time for which the data is stored in the node (Farmer) that provided the storage, and the volume of transactions.

Process of uploading data

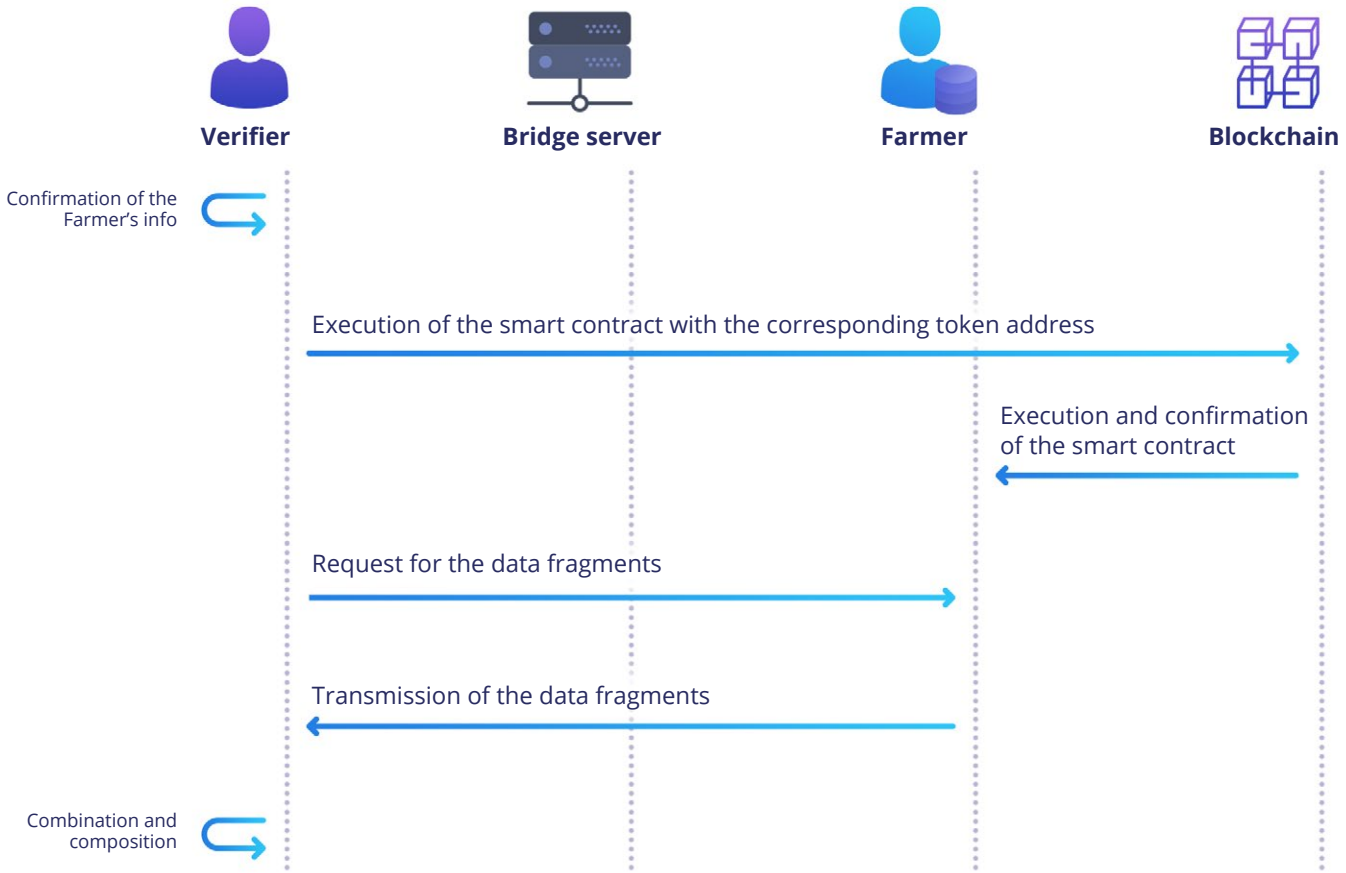
A node that attempts to store data (the Verifier) encrypts the data and then breaks it into fragments of a set size. It then requests information on a Farmer from the Bridge. The Farmer will generate a smart contract associated with the data, and will have the token address.
The Bridge transfers the token address and IP address of the Farmer that is best suited to the Verifier. The Verifier uses the Farmer's IP address to transfer the corresponding piece of data to the Farmer, who stores it, and executes the smart contract using the Farmer's token address. The Bridge constantly monitors whether the Farmer has correctly saved the data, and periodically checks the accuracy of the Farmer's data after that.
After confirming that the data was correctly stored, the Bridge transfers the information about the stored data fragment to the Verifier. Once that is done, the Farmer will receive a reward based on the size of the data stored in the Farmer's network, the time that the data is stored, and the number of data transactions.



Process of downloading data

The Verifier acquires data for downloading from the information on the data fragment received from the Bridge when saving the data.

The information on the Farmer storing the Verifier's data fragment is saved in the Verifier's network. In order to download the data, the Verifier executes the smart contract using the Farmer's token address. This means that coins are also payed when data is downloaded from the Farmer's network. The Verifier downloads the data fragments from the Farmer using the IP and token addresses and combines them, then decodes the data to obtain the original data.



3. About Gas and the PoSTT fee

All transactions and smart contracts processed in the PoSTT blockchain can be seen as scripts. For example, looking at a simple transaction, transactions can be seen as a combination of opcodes. The meaning of the opcode is the minimum unit constituting the script of the transaction. As an example, when we see the instruction “Push PublicKey”, it is a simple command to enter the PublicKey to the stack.

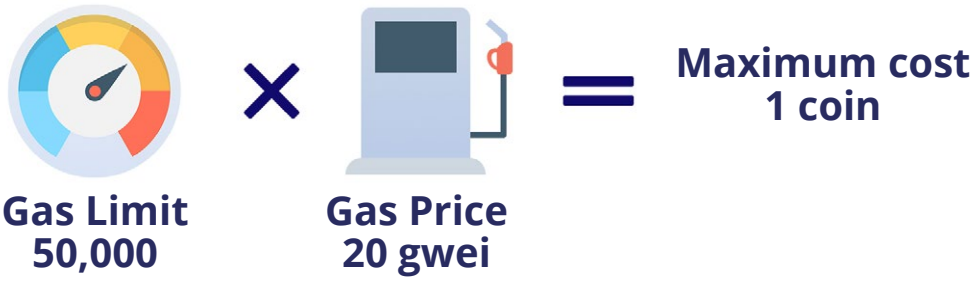
In this case, the transaction, being a combination of instructions as seen above, can issue the verification code of the transaction as a script. This script is executed by the virtual engine on blockchain, and can confirm the accuracy of the transaction as the execution result of the script.

Here, Gas is the amount of coins necessary to execute the opcode, which is the smallest unit constituting the script of the transaction. Both transactions and smart contracts can be seen as a combination of opcodes (i.e. as scripts).

In other words, Gas can be seen as the cost of processing the opcode, which is the smallest execution unit constituting the script.

Why is Gas necessary?
When there is no Gas, that is, when there is no cost to execute the opcode, a malicious attacker can destroy the virtual engine on blockchain by inserting code that will repeat infinitely in the script. By adding a cost-per-execution unit to prevent this, it is possible to prevent various malicious attacks by adding expenses proportional to the length of the script command.

How is the commission calculated in the PoSTT blockchain?
In the current PoSTT blockchain, 10^15 wei is equal to 1 coin.
1 gwei is 10^9 wei.



3. Technology

Let's assume that the Gas Price (gas price) is 20 gwei. Users do not know the exact number of op-codes for transactions when generating the transactions. We will introduce a value called the Gas-Limit. One Gas corresponds to one opcode. The user sets the GasLimit to 250 and generates a transaction. In this case, the user will pay only 250 * 20 gwei as a commission.

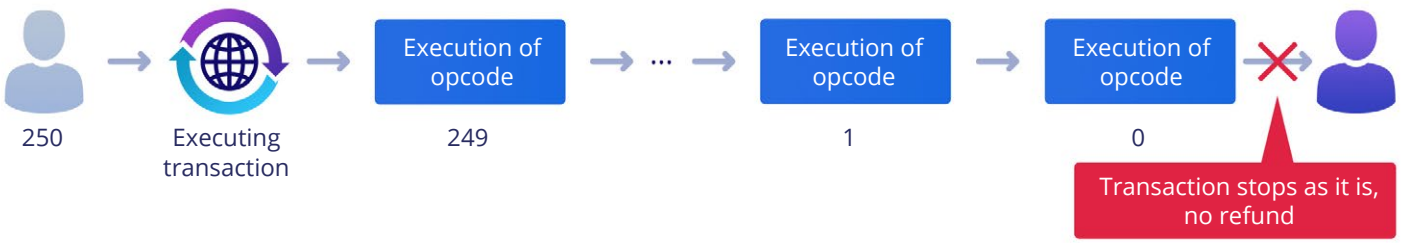
If the number of transaction opcodes is actually 80, then 250-80 = 170, so 170 will not be used. In this case, the cost corresponding to 170 * 20 gwei will be returned to the creator of the transaction.

As a result, the actual fee is only 80 * 20 gwei.
The following chart reflects the example above.

In the above example, the user sets the GasLimit to 250 to generates a transaction, and the actual gas required does not exceed 250.

However, the gas actually required for transactions may exceed the GasLimit set by the user. Let's assume that the user has set the GasLimit to 250 for the transaction, but the actual required gas exceeds 250.

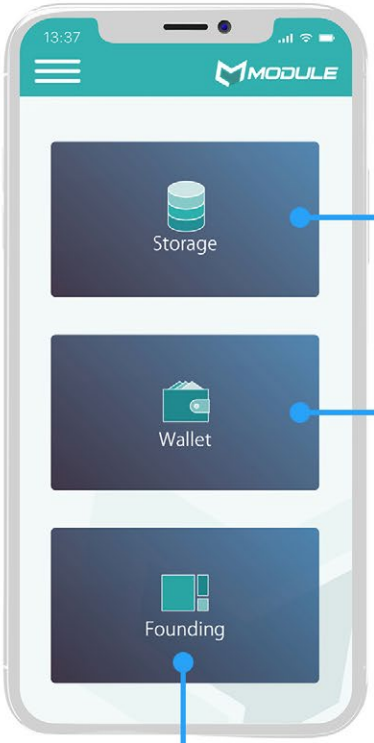
In this case, the transaction will end without being executed, and coins corresponding to 250 gas will not be converted for the sender (= the user who generated the transaction).



There is one more problem which must be considered. It is the problem of compensation for the Miner. In other words, the actual fee will be the "number of opcodes * gas price + the miner's fee".

4. MODULE App

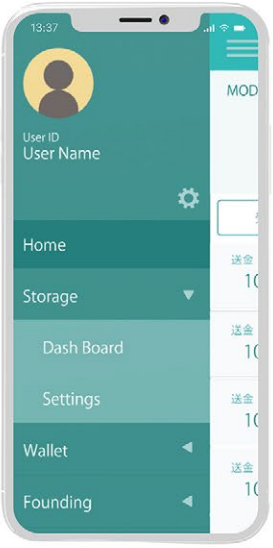
MODULE App image



Information on the storage space of the device, lended storage, time, etc.

Graph explaining the number of tokens mined, lended storage space, time, transactions

"Founding" model (see next page for more information)



Storage and verification of tokens; management of deposits and withdrawals

*All screens are under development. Actual services may differ

5. About the utility token

“Founding” model

6. Use cases

MODULE App — data storage service

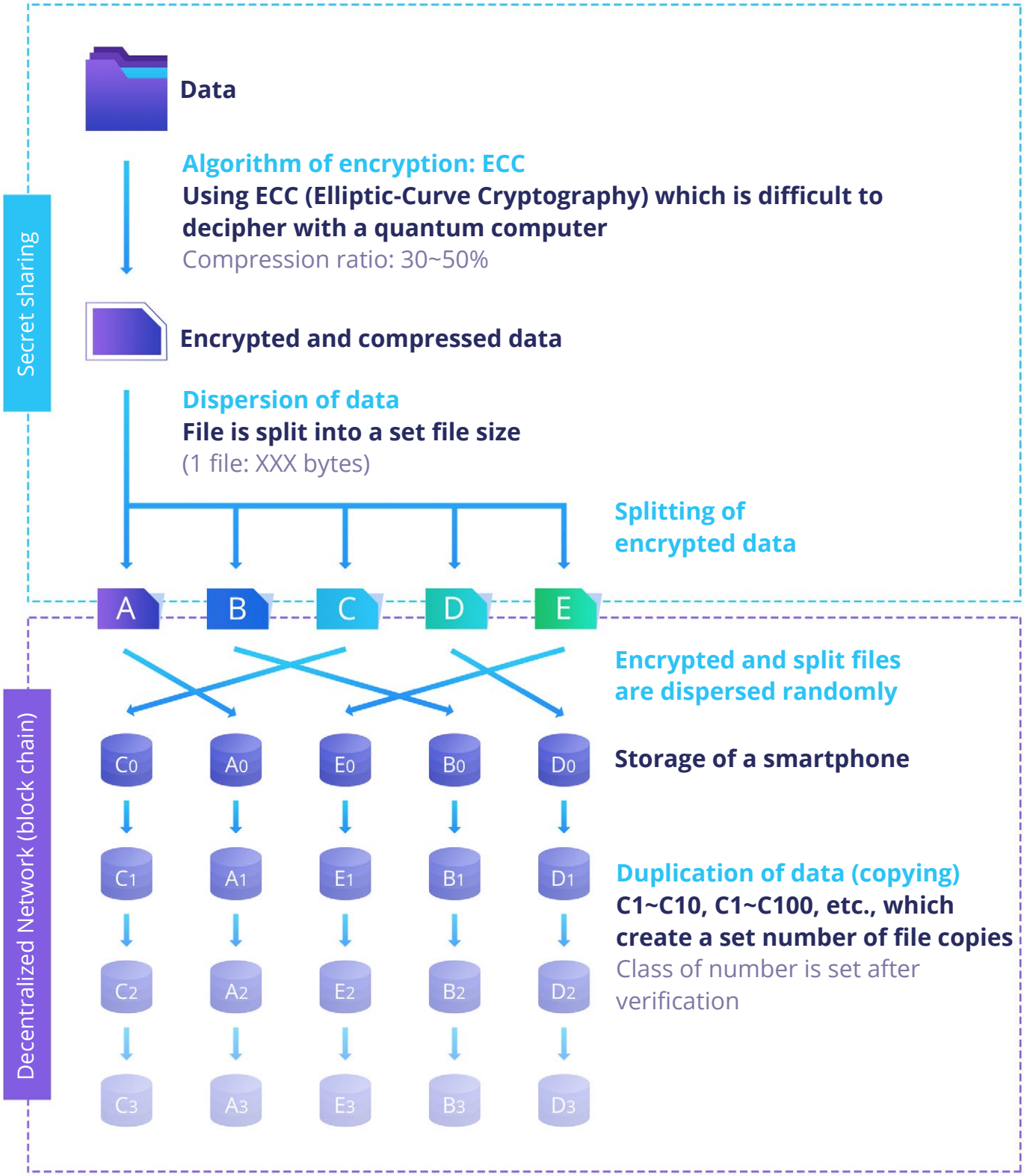
MODULE is suitable for storage of sensitive information because its distributed storage keeps data in fragments in many different places. It can be used to store information that should be kept secret from others.

In particular, by storing information in a distributed store like MODULE, one can enhance information security through “secret sharing”. In other words, if sensitive information is divided into fragmentary pieces of information and stored in separate places, information cannot be reproduced with only one fragment, but if several pieces are gathered, the information can be reproduced. This Secret Sharing method will be used in blockchain, and to build secure cloud storage for the safe storage of sensitive information.

The technique for concealing documents recorded in blockchain through the management of secret sharing keys has already been developed. One obstacle to utilizing blockchain to handle sensitive information was the fact that information on blockchain must be disclosed to the entire community of users. However, by combining blockchain technology and secret sharing, one can expect higher security and convenience. In this way blockchain can be used in various fields such as finance, distribution, in the supply chain, official document management, etc.

6. Use cases

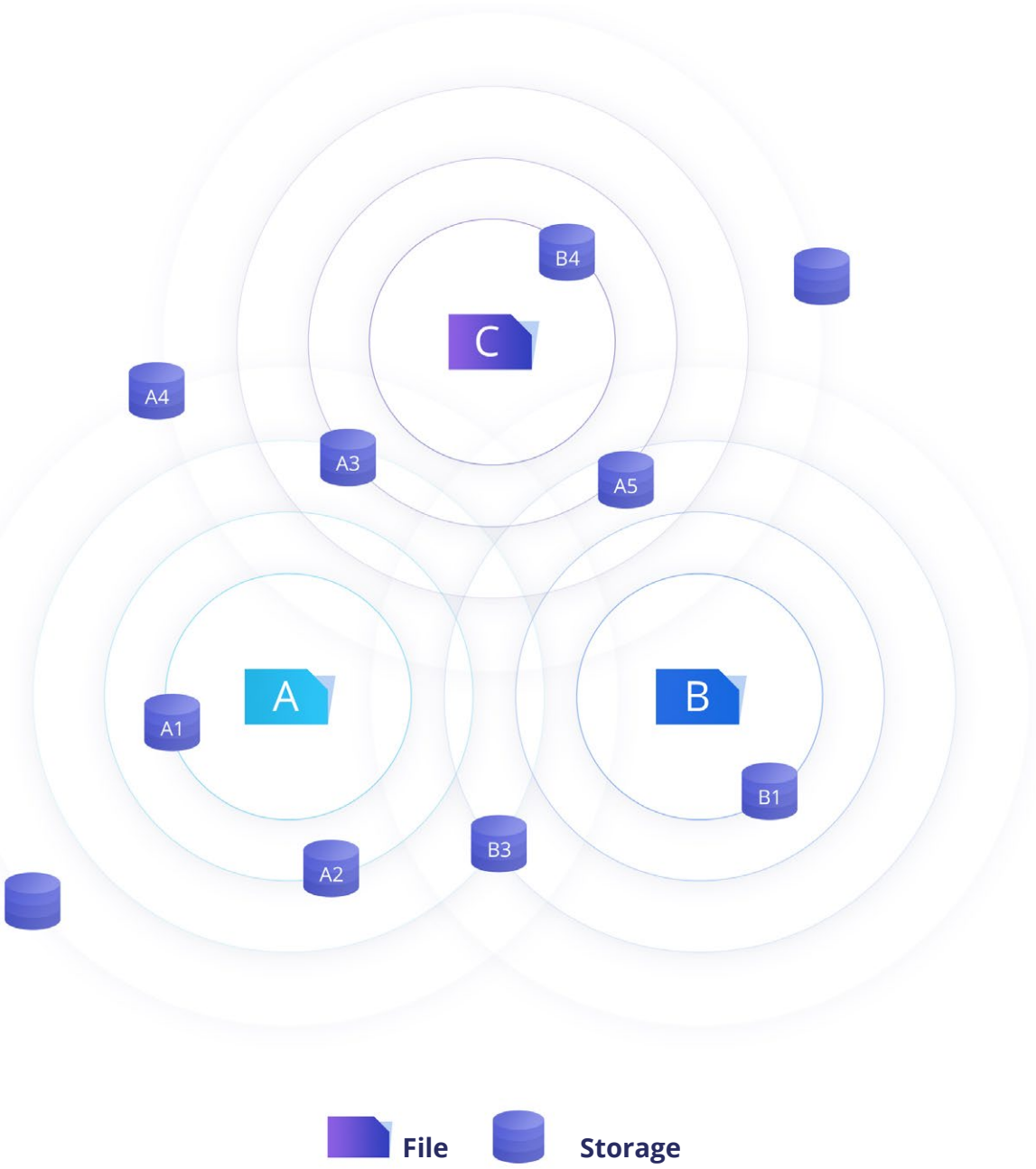
(Encryption, separation, distribution of data)



6. Use cases

(Data distribution)

Spreading files from the storage devices which are the closest to distributed files



7. Token

Token - MODL

Ticker symbol:	MODL
Token during ICO:	ERC-20
Type:	Utility token
Total emission:	15,000,000,000MODL
Price per 1 token:	1MODL = 0.008 USD

Softcap:
$ 5 000 000
Hardcap:
$ 18 000 000

Total emission:
15,000,000,000 tokens
For distribution:
2,250,000,000 tokens

Token allocation

15% public sale	15% team& advisors	5% private presale	5% ICO incentives	60% mining

8. Marketing strategy

The goal of the project is to create the Module economic zone. To use a publicly available blockchain to connect the world

PHASE 1

MODL App — development of the product

- Internal testing of the beta version is planned for October 2018

  After testing is finished, the beta version will be distributed in December
- Official release in Google Play, App store in January 2019

PHASE 2

The value of MODL PF is tied to the number of downloads

- A feature of our project is that a token holder is automatically a MODL user The beta version of “MODL App” will be distributed to users who purchased MODL tokens, and the value of MODL will grow along with the number of downloads of the application.
- The App will be distributed with the help of influencers to maximize user acquisition. Press release in Asia is planned for August 2018.

PHASE 3

MODL PF operation

- Advertising model, crowdfunding, etc. We will release unique content in which users can participate.

PHASE 4

Expansion of the economic zone through token economy

- The Module economic zone will be created through the acquisition of users and expansion of content worldwide.

9. Road map

May 2018
Management of the token sale
Participation in Consensus 2018
Start of Module platform development
Start of MODL App development

July 16, 2018
Start of presale

July 31, 2018
End of presale

August 1, 2018
Start of ICO

September 30, 2018
End of ICO

October 2018
Listing on exchange
Start of development of the Secret Sharing service

October 2018
Building of mining server
Testing of MODL App beta version

November 2018
Testing of Module platform

December 2018
Start of Module platform operation
Distribution of MODL App beta version

January 2019
MODL App in Google Play and App Store

10. Team

Engineering

Toshiki Tashiro

Alam Jahangir

Honbo Kei

Mitsugu Saito

Takuya Yamagishi

Jack Lee

Masafumi Watanabe

Hiromasa Saito

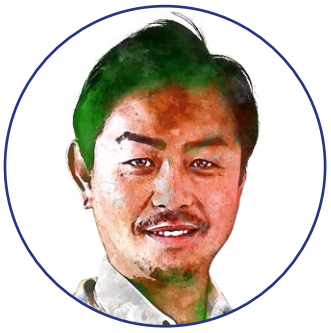
Yoshimitsu Tsukui

10. Team

Management

Yoshitomo Kikuchi
Marketing

Yuichi Yoshida
Marketing



Eisuke Matsumoto
Marketing

Koji Takane
Technology

Marina Kazakova
Press

Advisors

Hiroki Owada
Senior Project Advisor

Seiichi Hosaka
Legal Advisor/General Counsel

Nick Evdokimov
BLOCKCHAIN ADVISER

Hiroki Kato
Marketing adviser

11. Risks

About Risks

It is strongly recommended that investors willing to participate in the ICO read and understand the following disclaimer and ICO risk factors before participating. Those living in countries where ICOs are prohibited cannot participate in this ICO. Those who have never owned a virtual currency.

- Those who have no knowledge of virtual currency;
- Elderly people over the age of 75;
- Individuals under the age of 18;
- Those who need guardians or custodians;
- Persons whose investment experience in securities such as stocks and bonds, derivatives etc. is less than one year;
- Residents of developed countries whose financial assets are less than USD 100,000;
- Residents of developing countries whose financial assets are less than USD 30,000;
- Those who intend to convert 50% or more of their financial assets into tokens in this ICO;
- Individuals whose identity/status is unclear;
- Those who try to impersonate someone else to join the ICO. This includes those who do not comply with the laws of their country of residence.

11. Risks

1. Price fluctuation risk

The price of the token depends on the performance of the token issuer, the success or failure of the business plan, current prices, the foreign exchange market, trends on the securities market and other markets, natural disasters, war, political changes, regulation enhancement. It may be influenced by the spread of other virtual currencies, or by unforeseen or extraordinary future events. The value of the token held by the customer may drop significantly compared to the purchase price or lose value if the business plan of the token issuer does not progress as planned or is abandoned, or due to poor management.

2. Funding at the initial stage of the project

An ICO is often performed to collect funds before or at the beginning of the project that the token issuer is planning to develop in the future. The success or failure of the project is often very uncertain at the token purchase stage, and if the planned project fails, the customer may lose all of the contributed funds.

3. Risks inherent in the issued tokens

Tokens are not legal currencies such as US dollars, British pounds, euros, Japanese yen etc. In many cases, there is no specific person who could guarantee its value. In addition, there is a possibility that risks, such as program bugs, are inherent in the token itself.

4. Liquidity risk

Transactions may become impossible or difficult due to market trends or the volume of transactions with tokens, or may be conducted at an unfavorable price. If a specific person does not guarantee the value of the tokens, the tokens may lose their value due to a fall in liquidity.

5. Risks of Cyber-Attack

There is a risk that account authentication information may be leaked due to a cyber-attack, and that the tokens held by the customer may be remitted without permission.

6. Risks posed by the network

Token transactions are not recognized until the completion of sufficient transaction confirmation (authentication of the transaction in blockchain), so the tokens will be on hold for a certain period of time. This may result in the customer's transaction not being reflected in the account managed by the customer, or in the customer's transaction being canceled before the transaction is successfully confirmed in the network. As the tokens are registered electronically and their relocation is performed by the network, there is a risk of their loss.

7. Risks caused by changes in legislative / tax systems

The laws and system of taxation of ICOs and tokens are currently changing. ICOs may be prohibited in the future, or the tax restrictions may be made more stringent due to changes in laws, regulations, tax systems or policies. There is the risk that the possession of and transactions with tokens will be restricted, or that the handling of tokens may be more disadvantageous compared to the current situation, and in this case customers may suffer unexpected losses.

8. Ohter risks (including, but not limited to the following)

There is the risk that a third party may masquerade as a token issuer, display an unauthorized virtual currency address, or try to fraudulently obtain the virtual currency bought by the purchaser.

- The terms “virtual currency” and “cryptocurrency” used in this document are synonymous in a broad sense.

12. Outro

Imagine that your smartphone, an indispensable part of your everyday life, becomes a machine.

By developing a new consensus algorithm called Proof of Space, Time and Transaction (PoSTT), the MODULE team proposes an innovative technology which will enable people all over the world to easily participate in mining. In a word, we want to bring more joy to this world through Module, and make the world a better place by developing this technology. There is no doubt that the innovative technology called blockchain and the IT sphere itself will continue to develop in the future. If it is actively used, the platform may replace existing database applications and content delivery services. We want to contribute to creating a world where anyone can make any ideas and services real. As a first step to creating this world, our team accepts the challenge of conducting an ICO.

MODULE is about to throw a big stone in the lake of the cryptocurrency market. The thrown stone will cause ripples, and when our thoughts take real shape and people get to know them, we will be able to make a change in the world.