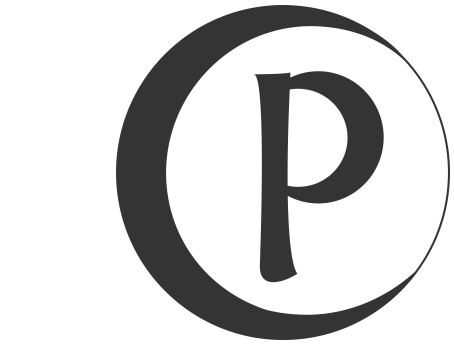


prajna paramita

White Paper

PRAJNA FUND

Version：V1.00

Update Time：2018.04.28

Official Website：www.prmichain.com

Abstract

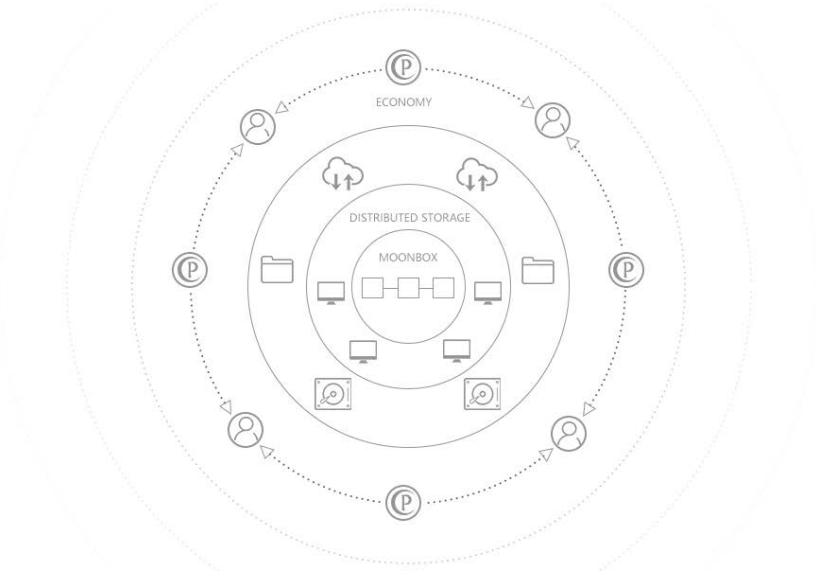
With the advent of the Internet & Blockchain Era, our network environment has been quietly undergoing a revolution: The Centralized Servers are being replaced by Decentralized Open Servers, the Trusted Participation being replaced by Verifiable Computing, The Vulnerable Locations Addressing being replaced by Flexible Content Addressing, the inefficient Integral Services being replaced by the Point-to-Point Algorithmic Market, and the feasibility of Decentralized Documentary has been verified by the emerging Blockchain technology. Meanwhile, the Client-encrypted Point-to-Point Cloud Storage network will allow users to transmit and share data without relying on the third-party storage providers. To cancel the Central Control will alleviate most of the traditional data transmission failures and outages, while significantly improving the security, privacy, and data control.

Prajna Paramita Cloud serves as a decentralized Blockchain-distributed and Cloud-computing service platform that turns the cloud storage into an algorithmic market. This market runs on a Blockchain with local protocol tokens. The miners on the blockchain can participate in sharing and exchange through their own storage surplus, bandwidth, files, and other data resources to obtain PRMI Awards. The cloud storage network offered by Prajna Paramita Cloud can provide security for the entire network process, as the content has been encrypted at the client end, while the storage provider and other users have no access to acquire the Decryption.

Prajna Paramita Cloud can provide the stimulus layer for the top level of IPFS above the storage infrastructure for any kind of data. It is useful for the decentralizing of data, building and running the distributed applications, as well as the implementation of Smart Contracts.

The Essentials of Prajna Paramita Cloud

Prajna Paramita Cloud is a decentralized Blockchain Distributed Cloud-computing service platform. Through the Prajna Paramita Chain, MoonBox (Distributed Hardware Terminal), Decentralized Storage Network, Point-to-Point Hypermedia Distribution Protocol Technology to achieve a global Distributed Cloud-computing platform. Thus, it serves as a Global-oriented, Point-to-Point Distributed Cloud Storage computing platform.



Background

In the past, Cloud Storage relied almost entirely on the large storage vendors as the trusted 3rd party providers to transmit and store data. However, there existed inherent weaknesses for the system under the trust-based models. Due to the encryption in client side not standardized, the traditional clouds proved to be vulnerable to a variety of security threats, including the middle-party attacks, malwares, and application defects, which also led to the inevitable explosion of consumer privacy and corporate data. In addition, in the times when universal access to the Internet becoming more and more popular, the Centralized Servers obviously cannot meet the thriving demands for Internet access globally.

The Development of Blockchain Technology

Since the birth of Bitcoin in 2009, Blockchain technology has appeared on the arena of history. The core advantage of Blockchain technology is that it no longer requires a traditional centralized organization.

By utilizing the technological measures of Encryption Algorithms, Consensus Mechanisms, and Time Stamps etc., Blockchain technology has realized the Point-to-Point transactions with coordination and collaboration in distributed systems that not relying on a certain credit center. The effect of which has enabled the avoidance of the prevailing data security issues, improved coordination efficiency, and enhanced the risk mitigation & control for centralized organizations.

During the recent years, people have conducted the innovative researches on aspects of Blockchain Decentralization, Consensus Algorithms, and Security Anonymity, such as: Graphene utilization, the enhancement of transaction performance by means of Lightning Network; the enrichment & improvement of consensus algorithms by Proof of Stake (POS), Delegated Proof of Stake (DPOS), Practical Byzantine Fault Tolerance (PBFT); the enhancement of transaction security by means of Zero-knowledge Proof (ZKP), and mixed currencies etc.

The Significance of Prajna Paramita Cloud

The Rational Utilization of Resources

Through the methods of decentralizing and files sharing, the problem of Resource Idleness for hard-disks and CPUs in personal computers has been resolved. The unused hard-disks and CPU resources of users could be collected and re-allocated, thus enabling the rational utilization of resources distributed in various places, which forms the application of ecosystem under the Prajna Paramita Chain .

The Advantage of Storage

By means of the Distributed Storage Technology, the waste of storage space has been eliminated, while the data can be automatically redistributed with all computing devices equipped with the same file system being connected together, thus improving the utilization of storage space. The principle is to use Content-based Addresses instead of addresses based on domain names. Which is to say, the content that the user has been looking for is not a certain address but the information stored somewhere. Therefore, it is not required to verify the identity of the sender, but only the verification of the content, which makes the web pages run faster and safer than before.

Improve Efficiency to Resolve Network Jam

The characteristics of relatively high fault tolerance, high throughput, proximity principle, and portability of Distributed Storage has enabled the retrieval of data more convenient that unrestricted with geographical limitations, thus greatly lowing the occurrence of error probability. Amongst the Point-to-Point transactions exists an autonomous agent that can perform such operations without the help of major Manual Interactions.

The Decentralized Network

The DSNs in Decentralized Network have been used as the storage provider to aggregate the global users and to provide the self-coordinated services for storing and retrieving data. This kind of coordination proved to be decentralized and no trust required: the verification can be implemented through the coordination of protocols and individual participants, thus enabling the system to obtain security operations. While the DSNs can use different coordination strategies, including Byzantine, Gossip, or CRDT, depending on the requirements of systems.

Prajna Paramita Chain

Prajna Paramita Chain serves as a decentralized distributed sharing system based on Blockchains and is used to form and execute storage contracts amongst the End-to-End & Point-to-Point transactions. The End-to End negotiation of contracts, , transmission of data, the verification on the integrity & availability of remote data, are all conducted on Prajna Paramita Chain, with data retrieval and content addresses available. Prajna Paramita Chain theoretically can achieve 1000TPS on usability performance by optimizing the block spacing, block capacity, and the consensus algorithm. Prajna Paramita Chain, as the core part of the Prajna Paramita Cloud platform, has performed the linkage on all terminals, thus allowing all network endpoints not only to act as browsers or clients, but also as operators of this network, making everyone as the server for effective operation.

Data Security

The data files shall be encrypted in the client by default and then stored on the storage node, which means that the person who stored the data actually has no visibility on the contents of data file.

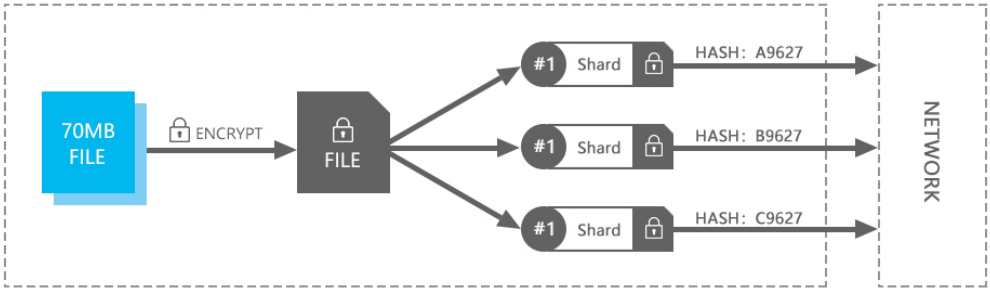
Whist for some sensitive data, the data owner can choose to use hardware encryption method to generate encrypted data file and then publish it to the nodes of Prajna Paramita Chain.

Prajna Paramita Chain requires that files be encrypted on the client before further sharing. The implementation reference uses AES256-CTR standard, whilst can also enable the converged encryption or the implementation of any other tunable systems. Such characteristics will protect the content of the data away from the data storing by storage providers. The data owner retains the full control over the encryption key, thus controlling the access to the data. The data owner can separately keep the data files and have the location information encrypted in the network. With the growing of fragments collections in the network, it will become more difficult to find any of the given shard collection without knowing their locations, which means that the security of the file is proportional to the square of the network size.

Fragment size is a negotiable contract parameter. To protect privacy, we suggest normalizing the fragment size to a multiple times of one byte, for example 8 or 32 MB. The standardized size prevents the side channel from trying to determine the contents of a given fragment and can provide mask for the fragmented flow under the network.

To fragment the large files (such as video contents) and to distribute shards across nodes have reduced the impacts of content delivery on any given node. Bandwidth requirements are more evenly distributed throughout the network for end users to utilize for enabling parallel transmissions.

Since peer nodes normally rely on separate hardware and infrastructure, thus irrelevant with data failures. The phenomenon means that to create a redundant mirror of the shard, or to apply a parity scheme across the shard set can be an extremely efficient way to ensure the feasibility of program. The availability is no denying directly proportional to the number of nodes that storing the data.



1. The file is encrypted.
2. The encrypted file is split into fragments, or multiple files that are merged into fragments.
3. To perform an audit preprocessing on each fragment.
4. Fragments can then be transmitted to the network.

Content Addressing

The Content-addressed Storage identifies a file by generating a unique hash value from the file's content, rather than by the location of saved files. Files with the same content will only have one copy existing in the system to save the storage space. The files are addressed according to the unique hash value generated by the stored data content, with good searchability, security, reliability and scalability.

Unlike structured data that needs constant changes and updates, the value of the fixed content comes from a combination of several features such as authenticity, longevity, high capacity, and online availability etc. Content Addressing can effectively cope with the massive fixed content information for efficient storage, data archiving, management, retrieval, and protection on the files.

No Duplicated Data： Since each content or data segment on the Prajna Paramita Chain is provided with a unique hash value, when the duplicated contents are stored, the same hash value shall be recognized by the system to avoid the storage duplication of the same content. This function not only saves a lot of space to improve storage efficiency, but also greatly simplifies the data management process.

Data Integrity： It is easy to implement WORM (write once, read many times) by giving attributes such as data retention time, so that the authenticity and integrity of data can be fully protected.

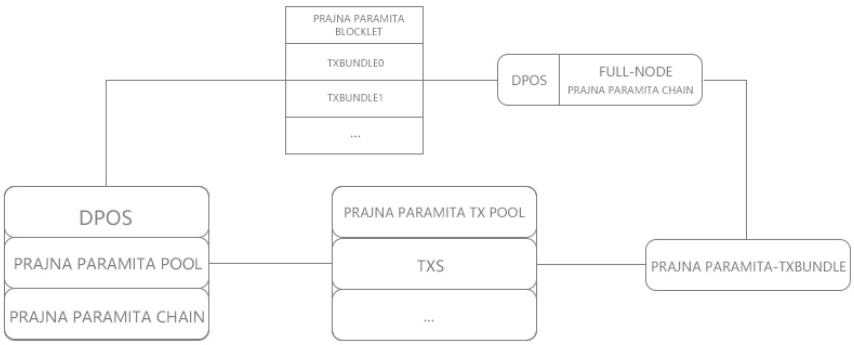
Improve Efficiency： To adopt independent node redundancy architecture and use multiple standardized servers as nodes to form a grid. Hence when a user accesses a certain file, a hash request shall be broadcasted, thus enabling the node storing the file been found and transmitted to the user.

Effective Cost Reduction： Prajna Paramita Chain uses the Near-line Archive Storage to logically store archived data through Cloud Computing. It can support large number of users for massive access and facilitate the centralize management to effectively reduce costs.

Prajna Paramita Chain effectively reduces the difficulty of understanding, managing, and manipulating the physical or logical

location of information on storage media through Content-addressed Storage; while using the modular hardware architecture to efficiently manage storage resources, keep the live transparency on users during the process. The application of Prajna Paramita Chain can meet the rigid requirements of availability, authenticity, long-term sustainability and manageability on the fixed content.

Consensus & Blocking



The Consensus & Blocking Mechanism is made up of the transaction package (Tx-Bundle) and Prajna Paramit Blocklet. This algorithm is based on the DPOS consensus mechanism. A transaction package

contains the transaction records of Prajna Paramita Chain. Whilst the full node generates and contains the blocks of different transaction packages which are published onto the block network.

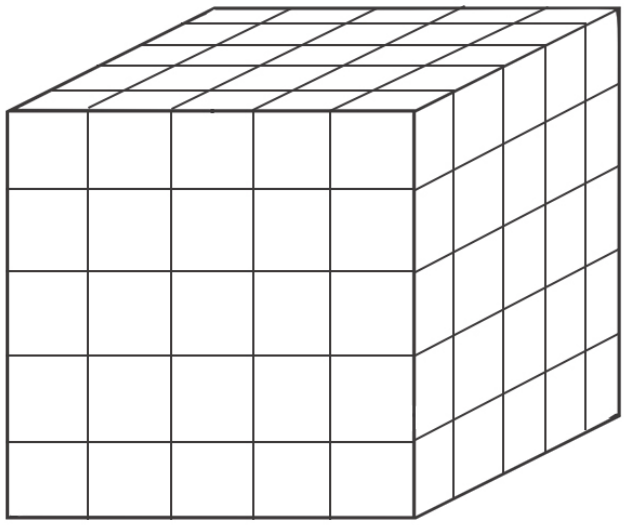
Information on the Chain

Not all data and information need to be published and stored on the chain. The objects stored on the chain is the content-addressable resources with the address tags. In addition to the basic block information, other objects stored on the chain involve: the accounting transactions, object data, storage transactions, certification transactions etc.

Decentralized Storage Network

In the application of decentralized computing, there is an epoch-making concept which is called the Inspired Decentralized Online File Storage System. Currently, if you want your files or data to be safely backed up in the cloud, you have three options: 1. Upload them to your own server; 2. Use a centralized application, such as Google

Drive or Dropbox, or; 3. Use the existing decentralized applications such as Freenet. However these methods have their own drawbacks: The first method has expensive setup and maintenance costs; the second method relies on a single trustworthy entity, and often involves significant price increases; while the third method proves to be slow and has very high limitation in space capacity for each of the users, since it depends on the user's voluntary contribution of the storage space. The motivated file storage protocol has the potential to become the fourth method, which shall motivate the executors (customers who store the user data) to become the nodes by network decentralization, thus providing the high-capacity storage and high-quality services.



To simplify, provided you have a 10 GB file and you want to spread it to the network. First of all, you shall encrypt the file, and then you split the file into 125 blocks. You arrange these blocks to form a 3D 5X5X5 cube, point out the polynomial for each axis, and then extend each axis, so that you can get a 7X7X7 cube at the end. You can find 343 nodes that are willing to store these blocks and only tell each node which entity information it belongs to that axis. In order to download the entire file, you shall make a request for all blocks and then see which block comes with the highest bandwidth. As long as the minimum number of blocks has been reached, you can use mathematical operations to decrypt the file and restore the file locally.

Decentralized storage is technically different from distributed storage. Decentralized storage is in a more isolated and untrustworthy network environment to meet a more secure, more trustworthy, and more controllable storage needs. Briefly, there’re three main goals for Decentralized Storage:

The first is Security. The traditional central storage is easily attacked by hackers. For example, the Bitcoin exchange in Japan has always been attacked by hackers for years. The banking systems of various countries have been attacked by hackers, and even in the case of inner piracy within the organization.Comparatively, the Decentralized

Storage will conduct the Data Cutting that scattered across the entire network. Hackers are unavailable toi attack all anonymous nodes on the entire network.

Secondly, it is Fast and Efficient, and although the centralized server is not close to all users, while Genaro's Decentralized Storage prefers the node closest to each user.

Finally, it is Cost-effective with Value Added advantage. Decentralized Storage Networks can form a trading market using idle or unused resources, the cost of which proved to be much lower than the centralized fixed cost. What's more, the sharers have the right for free bids in order to reach a minimum price, and the individual user can also customize and set different security levels for each file storage with different costs.

Kademlia Protocol

The design of Prajna Paramita Chain requires the construction of a Peer-to-Peer (P2P) network with many users and the nodes included can join and leave at any time.Therefore, a good routing table maintenance and search algorithm are very important.The Kademlia

Protocol is used as a basis to build the P2P (Peer-to-Peer) network. Generally, Kademlia uses the XOR algorithm to build a distributed hash table based on distance metrics, which can greatly improve the speed of route query. This proves to be significant for a Prajna Paramita Chain network with a large number of storage nodes.

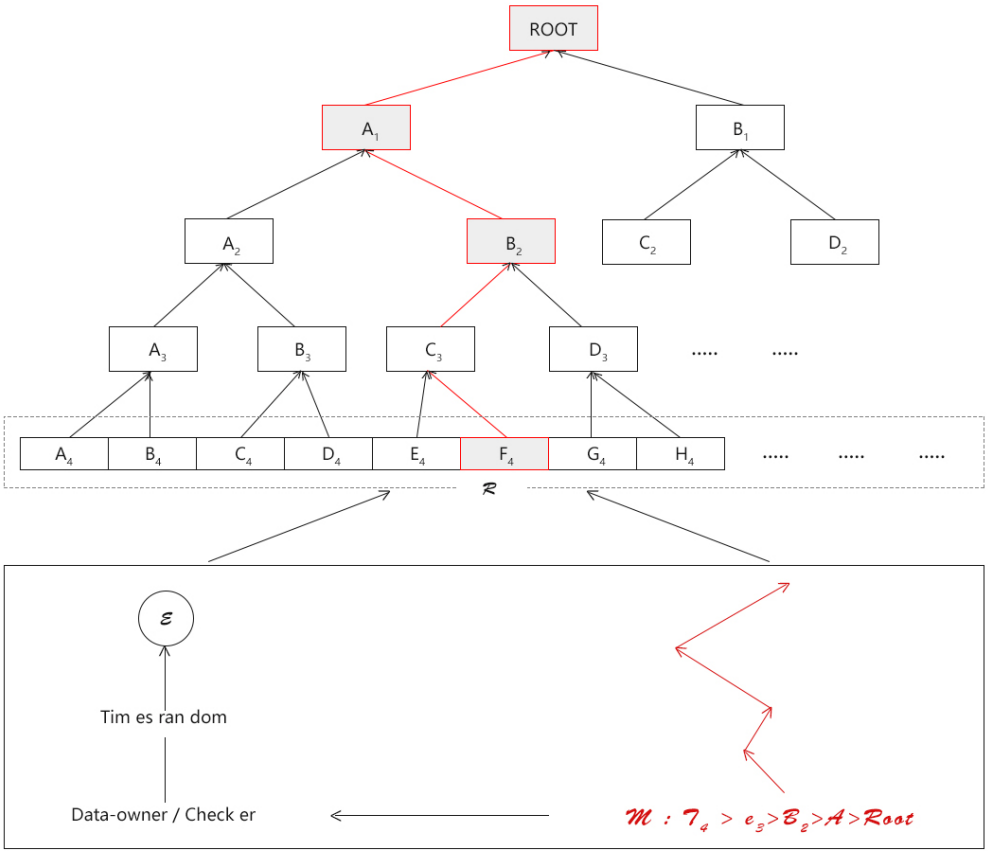
The implementation of the Kademlia Network will be mainly divided into two steps. Hence we will firstly build a P2P network based on a simple routing table and complete the Kademlia Network development while opening the storage node clients. While the node list maintenance of K-bucket in the Kademlia Protocol is exactly in line with our on-line requirements for nodes, but in the future it may be based on the credit rating of the docking points in the POC as a weighting value for sorting and swapping to help the observer select the closest nodes for verification, so as to adjustment the data distribution.

Storage Certificate

Merker Tree and Zh-Snark were introduced to form POR (Proof-of-Replica) and POST (Proof-of-Storage & Time) as the Quantification Documents issued by the Storer. While the storage nodes with high credit ratings are allowed the to provide proof within shorter time by

using POR, and the nodes with lower credit ratings are required to provide proof of storage market by way of POST.

Proof-of-Replica



The data owner can request a corresponding backup certificate from the Prajna Paramita Chain network at intervals:

◇ The data owner generates a check digit number C based on time and sends it to the Prajna Paramita Chain network;

◇ The storer needs to find the corresponding data fragment from the check number C and generate a → Merkle Check Tree.

◇ If the check passes successfully, the Prajna Paramita Chain network will update the Store-Book and the Reward-Book, while also unlock partial of rewards in relevance of such transaction in the Store-Book as compensation for storage.

Storage Market Proof-of-ST (Storage and time)

Although POR can guarantee that the data storer to save data at least for once, but can not avoid the evildoer to maliciously deceive. Please consider the following scenarios:

1. After the registrant backs up the data as required for the first time, it computes the Merkle checksums for all the data cutting and splitting sequences, and then deletes the data fragment files to save only the Merkle Checksum Tree.

2. After receiving the certification instruction, the storer shall request the other nodes that saved the data backup to obtain the data, and then calculate the corresponding C (→ Merkle) tree.

3. In the above scenarios, the perpetrators can obtain storage compensation by using extremely low calculation and storage costs. Therefore, the introduction of POST ensures that the Merkle Checksum cannot be calculated correctly if the data storer does not store the data fragmentation file, and no compensation can be obtained:

◇ Generate a sequence of entropy values S after the data is cut into pieces, and then generate hash value R using S and data pieces.

◇ The data owner sends the Sx (time-based entropy, globally unique) to the Prajna Paramita Chain network at regular intervals. The storer needs to calculate Rx from the Sx with the corresponding data fragments, and generate the corresponding Merkle Check Tree based on the Rx.

With the sequence of pre-entropy values, it is also possible to perform data inspection by the observer agent. The owner of the data can provide a sequence of entropy values to be passed to the

observer, who will then complete the POST verification check. In order to perform more safely, we will rely on the smart contracts to implement the agent check logic in future.

Proof-of-Credit

In the Prajna Paramita Chain Agreement, the credit certificate is bound to the account. The specific rating system varies according to different clients:

◇ Storage nodes: total storage, storage duration, online duration, and penalties

◇ All nodes: maximum transaction throughput, block-out speed, branching convergence speed, and online duration

◇ Observing nodes: Indexing service performance, online duration

◇ Data Owner: Storage data volume, transaction volume

◇ Attestation: Proof

Consensus Mechanism

Due to the nature of distributed storage, the blockchain needs a

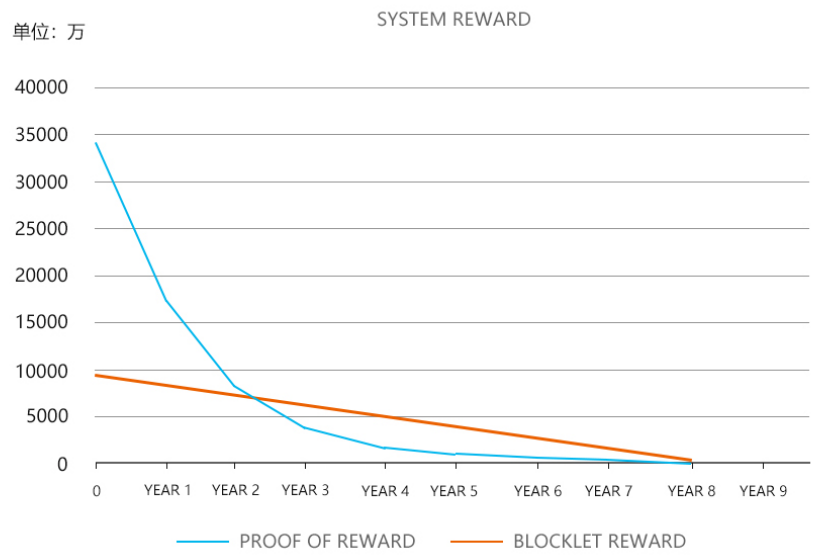
Consensus Mechanism to function properly. Prajna Paramita Chain selects the DPOS Consensus Mechanism, since DPOS does not need to spend additional computing power to achieve the distribution of interest after the production of blocks, whist it can also dynamically determine the execution results of smart contracts verified by the agent or the entire nodes according to the status of the network transactions.

The Token holding Prajna Paramita Chain can not only obtain the basic services in the Blockchain such as contract release and network fork, but also participate in voting and have the opportunity to become a Proxy Node to provide the services and acquire the Token rewards accordingly. Prajna Paramita Chain has named this Token as PRMI. Each AAC holder is called an equity person, who allocates the corresponding voting weights according to the number of PRMIs held. The agent nodes are selected by the equity holder. The first 31 winners with the most votes shall become the deputy nodes, which in turn help to authenticate the transaction. The order of work is determined by the number of votes, whilst the agent nodes can earn income if working normally. Provided it's working abnormally or not functioning well, it will be punished.

Reward and Punishment System

System Reward

The Prajna Paramita Chain network aims to encourage more nodes to join and construct a more robust ecosystem. The system rewards each of the contributing nodes as illustrated below.



Blocklet Bonus

The block time internal is set to 5 minutes (the fastest one can produce a block each 10 seconds). Thus 288 blocks can be produced

a day and 105,120 blocks per each year. For each Prajna Paramita Chain produced by the blocker, the Mine pool node can get 1623 PRMI awards, Each miner gets rewards based on the calculated power value and the overall power of the mine pool; while the awards halved for 105,120 blocks' production;. It is estimated that 340,000,000 PRMI awards shall be issued within 8 years.

Certification Rewards

The Prajna Paramita Chain network has reserved 80,000,000 PRMIs as the rewards for certifiers, motivating and inviting trusted organizations or institutions to serve as the certifiers, thus providing certification services for data on the chain.

System Punishment

Prajna Paramita Chain will systematically penalize the situations that causing ecological damage, including to deduct the rewards PRMI and to reduce their credit ratings correspondingly.

Data Lost

No longer pay for subsequent rewards for storage of data. Decrease its credit ratings. Once the threshold is reached, the user shall be blacklisted and cannot be re-connected to the Prajna Paramita Chain network any more.

Malicious Attack

Whether a malicious attack deliberately conducted without the block production, or to obtain a large number of PRMIs through abnormal means, the Prajna Paramita Chain network and the program will trigger the highest level of punishment: the node and all associated users shall be blacklisted and cannot be re-connected into the Prajna Paramita Chain network, while all the PRMI currencies on this account Shall also be collected accordingly.

Fraud

When fraud behaviors discovered, it's always too late to recover the losses, and there is no effective way to retrieve the payment & rewards issued by the system. Only by lowing the credit ratings, thus decreasing to the threshold, can the user be blacklisted without any privilege to re-connect to the Prajna Paramita Chain network anymore.

Smart Contract Mechanism

Smart Contracts allow users of Prajna Paramita Chain to spend tokens to request storage/retrieve data from the market and verify the proof of storage. The user can interact with the Smart Contract by sending

the transaction to the account to trigger the function within the Smart Contract;. We have extended the Smart Contract system to support the specific operations in the Prajna Paramita Chain. (eg, market operations, certification verifications etc.).

The Design Principle of Prajna Paramita Chain

◇ Unreliability Assumption of Nodes: The structure of the blockchain-based centralized network organization has allowed the single point of failure to occur and nodes to be unavailable during a short period of time;

◇ Ownership and Privacy: Data owners have ownership and full access to data, which are encrypted and private. The other roles can access and use the data after the owner's authorization;

◇ The Quantifiable Degree of Contribution: The degree of contribution of all parties involved in the agreement should have corresponding quantitative standards with contributions that can be observed. Such as POST and POR as a quantitative proof of storage space and storage time;

◇ The Consistency of Final States: Data objects are allowed to be in different states on different nodes, but their states can be quickly converged to obtain the consistency of network-wide nodes;

◇ Detectability and Recoverability: Can detect the availability of the entire network and the state of the entire network of data objects, and autonomously repair to a certain extent according to the strategy;

◇ Auditability and Regulations: A certain degree of supervision and audit may be conducted in certain specific areas or scenarios, provided that the data owners acknowledge and permit the action;

◇ Extensible APIs: APIs that are highly scalable and easy to use;

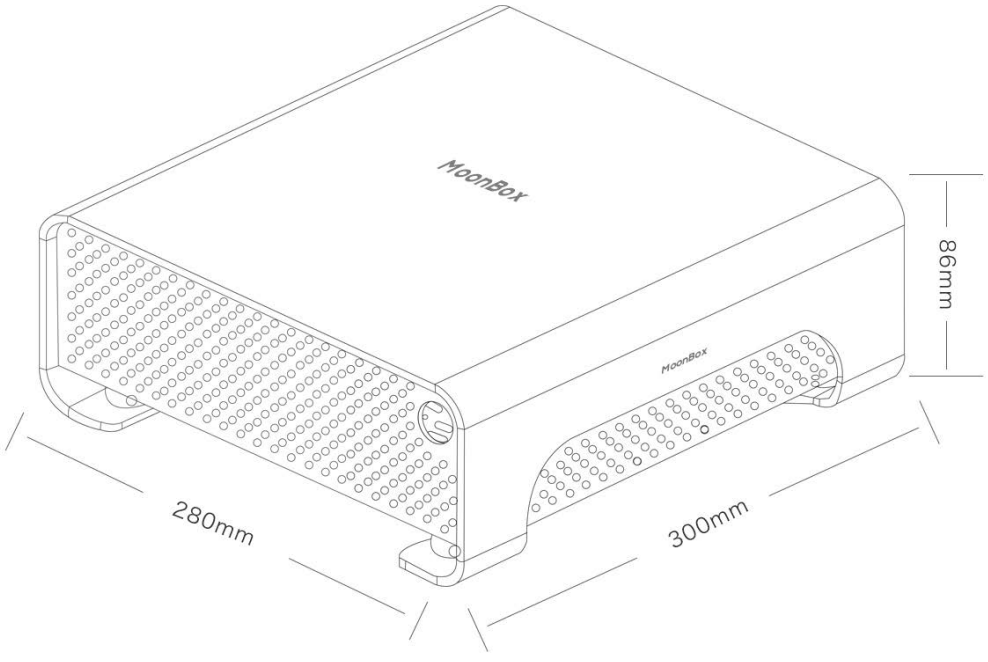
◇ Consensus Mechanism: The Consensus Mechanism based on DPOS

MoonBox Introduction

MoonBox is a hardware product based on Blockchain technology. It serves as the universal hardware host that creates the reward systems for users through Smart Contracts. With internal 128GSSD hard disk storage and the optional external hard disk storage devices, we provide comprehensive and stable CDN services for the Internet business based on the idle & unused resources provided by users. It combines series of innovative functions for the downloading

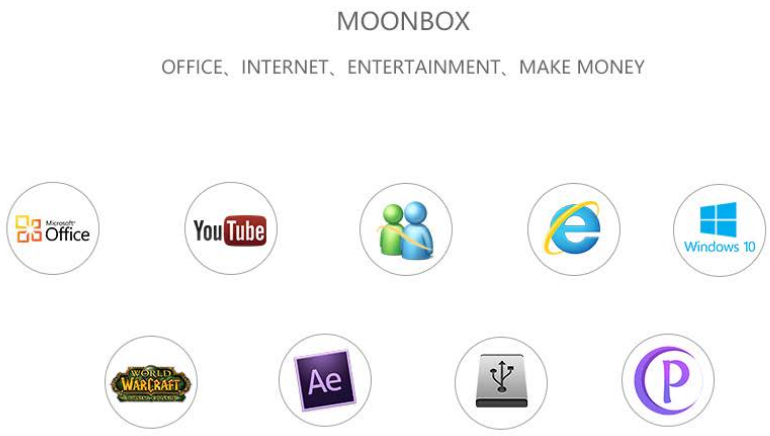
platforms, UGC acceleration platforms, streaming media platforms, and the dynamic acceleration platforms with value-added services to accelerate their business expansion. The Prajna Paramita Cloud will open more massive service capabilities in the future to provide users with CDN acceleration services that meet the needs of the blooming Internet business. Users can earn PRMI currency by participating in the Prajna Paramita Chain nodes by sharing the unused storage space and bandwidth of the MoonBox.

As one of the core parts of Prajna Paramita Cloud, MoonBox will become the key node of Prajna Paramita Cloud. With the development of the number of nodes, Prajna Paramita Cloud's distributed cloud space will be enlarged and enhanced to realize a more functional Distributed Cloud Computing System to enhance the value adding for users.



The design size of Moonbox is only 300mm * 280mm * 86mm, which is more mini compact and portable with the fashionable appearance. Not only has Moonbox been designed with powerful functions to deliver excellent performances, but also equipped with characteristics for quiet operation, environmental protection, office & home applicability, and easy for mining functions.

Application Scenario



Office, Internet, Game Entertainment

MoonBox is a hardware device based on Win10 system that integrates the functions such as office, internet and games.Whether for daily office software, drawing tools or high-performance games,MoonBox

can all be easily controlled with excellent performance. The compact body, good built-in quality, high-speed computing power, extremely fast data reading speed and strong software compatibility features have enabled modern corporate offices a more convenient and environmentally friendly place to drive high production with efficiency.

Shared Storage

MoonBox provides the massive, secure, reliable, low-cost CDN cloud storage service that provides solutions to increase data storage and reliability. Users can open the MoonBox link network for storage and online visiting through Internet access. While the external hard disk devices can be used to expand the capacity with more flexibility. What's more, multiple storage types can be selected and used to fully optimize storage costs.

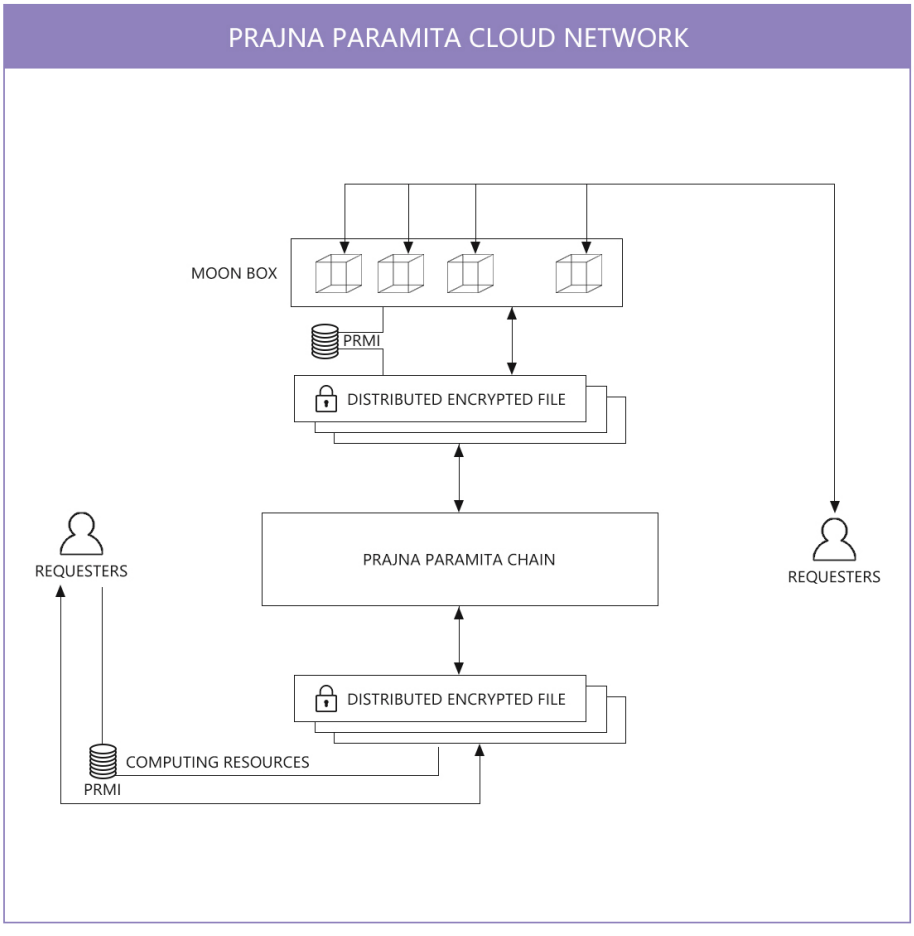
Get PRMI Awards

MoonBox is based on ecological stimulation mechanism for terminal nodes of Prajna Paramita Chains. Users can contribute their own free and unused space, bandwidth, and computing power to get the relevant PRMI rewards.

Prajna Paramita Cloud Ecology

Prajna Paramita Cloud is a decentralized Blockchain distributed Cloud-computing service platform. Through the Prajna Paramita Cloud, individuals can share their remaining space, bandwidth and traffic to participate in the sharing and exchange of data resources. Each ordinary user can become a resource node under the centralized shared cloud computing system and receive the block rewards — PRMI currency.

Prajna Paramita Cloud Overview



The Prajna Paramita Cloud platform uses Fog Computing as its core mechanism, and Fog Computing is a paravirtualized service computing architecture model. Compared with Cloud Computing, the Fog Computing architecture is more distributed and closer to the edge of the network. Overall, Fog Computing has concentrated the data, data processing and applications on devices at the edge of the network, instead of storing them almost entirely in the cloud, as Cloud Computing performs. The storage and processing of data largely rely on the local devices, rather than the servers. Therefore, though Cloud Computing is a new generation for Centralized Computing, while Fog Computing proves to be a new generation of Distributed Computing, in line with the "Decentralized" characteristics of Blockchains.

The Fog Computing is based on the small clouds, such as Personal Cloud, Private Cloud and Enterprise Cloud etc. The Fog Computing stands out by its quantity and emphasizes on quantity. No matter how weak a single computing node is, the Fog Computing function can access the node and conduct the data storage services without users' being connected to the remote large data centers. Generally, there are several obvious characteristics of Fog Computing: Low latency and location awareness, wider geographical distribution, mobility-adapted applications and the compatible support for more edge nodes. These features make the deployment of mobile services more convenient and can satisfy a wider range of node access.

The main goal of Fog is to increase efficiency and resolve the traffic congestion that may occur when it is transmitted to the cloud for calculation and storage. The devices for data generation and collection do not have the computing power and storage resources to perform various advanced analysis calculations and machinery learning tasks. Therefore, the Fog can have its own functions performed since it's operating on the margin of the network and in a sense also closer to the Cloud. While the Cloud servers have all the features needed to complete these projects, but they are often too far away to provide the in-time assistance. However, since Fog makes the endpoints closer with each other and accumulated together, the data storage can also be shared better.

The Fog Computing adds another layer between the terminal and the data center, which is called the Network Edge Layer. If you add a small server or reasoner with memory, some of the data that does not need to be put into the "Cloud" shall be directly processed and stored at this layer to reduce the pressure of the "Cloud", so as to improve the overall efficiency, and increase the transmission rate with delay effectively reduced.

With distributed Fog Computing, the Data Transmission Bands are formed among different devices through smart routers and other technologies & devices, which can effectively reduce network traffic and to release the data center's computational load.

The Fog Computing can be used as a calculation processing between the M2M (Machine-Machine dialogue) network and the Cloud Computing to cope with the large amount of data generated by the M2M network. The processing program is used to preprocess the data to enhance its usage value.

Prajna Paramita Cloud provides the shared computing service that can be exported to enterprises based on P2SP technology. Prajna Paramita Cloud will apply the Blockchain technology to establish a rather fair and transparent reward mechanism to encourage ordinary individuals to participate in the sharing and exchange of data resources. This will enable shared computing services provided by Prajna Paramita Cloud to be completely open to individual users, who can become the nodes for shared resources in the decentralized Cloud Computing system and earn the benefits from this system.

The Features of Prajna Paramita Cloud

Reliability

Prajna Paramita Cloud has a wide geographical distribution. In order to serve users in different regions, the same service will be deployed in each regional block point, making the High Reliability as an intrinsic attribute of Prajna Paramita Cloud. Once an area has abnormal services, users' requests can quickly be transmitted to other nearby

areas to get the related services. In addition, as Prajna Paramita Cloud has reduced the amount of data sent to and from the Cloud, the Security and Reliability features can also be further enhanced.

Convenience

Prajna Paramita Cloud supports high mobility, thus mobile phones and other mobile devices can communicate directly with each other, signals do not have to go around the Cloud or even surround the base station for circles ! In addition, Prajna Paramita Cloud also supports real-time interaction, diversified hardware and software devices, as well as the cloud-based online analytical calculations.

Low Latency

Prajna Paramita Cloud has a lower position in the network topology with a smaller network latency (total delay = network latency calculation delay), which proved to be more responsive.

Distributed

The Prajna Paramita Cloud architecture is distributed and closer to the edge of the network, where the data storage and processing are independent of cloud servers.

The Working Mechanism of Prajna Paramita Cloud

The services Prajna Paramita Cloud provides to users are the use of all facilities, including the processing, storage, networking, and other basic computing resources. Users can deploy and run any software, including operating systems and applications. Prajna Paramita Cloud provides server services, CDN acceleration services, file storage services, and data exchange services to individuals or Small and Medium Sized Enterprises (SMEs) through the distributed cloud storage at a relatively low storage price.

Computing

A set of controllers will be used to manage the entire life cycle of a virtual machine for a single user or group of users, providing virtual services based on the user demands. It will be responsible for creating, booting, shutting down, suspending, adjusting, relocating, rebooting, and destroying virtual machines, as well as to configure the CPU, memory allocation and other information specifications.

Persistent Object Storage

Prajna Paramita Cloud is based on the Content Addressing, Point-to-Point Hypermedia Protocols,thus capable of features as the high fault-tolerance, scalability with much saferand more open object storage, to

provides the persistent mirror storage for Glance and volume backup for Cinder.

Identity Service

Keystone shall provide the functions as authentication, service rules, and service tokens for OpenStack, thus managing Domains, Projects, Users, Groups, and Roles.

Network & Address Management (Network)

To provide cloud computing network virtualization technology for OpenStack & other services to enable the network connectivity. With the interfaces provided, users can define the Network, Subnet, Router, and to configure DHCP, DNS, load balancing and L3 services. While the network supports GRE & VLAN and the Plug-in Architecture supports many mainstream network vendors and technologies such as OpenvSwitch etc.

Block Storage

To provide a stable data block storage service for running instances. Its plug-in driver architecture facilitates the creation and management of block devices, such as creating volumes, deleting volumes, the mounting and unmounting volumes on an instance.

Data Transfer

The data shall be transmitted via Prajna Paramita Chain. Users can expose the endpoints where the Client applications may upload or download fragmentations. The client's requests are authenticated by the tokens provided by the previously delivered messages after data retrieval.

Network Access

Data owners must bear the burden of network access to maintain the availability and integrity of data on the Prajna Paramita Chain network. Since the nodes cannot be trusted, the set of challenges of hidden information security cannot be outsourced to an untrusted peer. The data owner shall be responsible for preprocessing fragments, issuing and verifying audits, providing payments, managing file status through the collection of fragments, management of files with encryption keys added etc.

Audit Payment

The miners will only receive payments when the network can audit whether their services are properly provided.

Development Route

2017 Q3

Project of Prajna Paramita Initiation

Q4 2017

Completion of MoonBox hardware design and internal structure construction;

2018 Q1

Prajna Paramita Chain Network construction and testing;

2018 Q2

MoonBox Client officially launched;

2018 Q3

The Prajna Paramita Cloud platform was built;

2018 Q4

The Prajna Paramita Cloud Beta went online to conduct Open Beta (OB);

2019 Q1

The official version of Prajna Paramita Cloud went live.

Prajna Paramita Token / Introduction to PRMI

On the Prajna Paramita Cloud platform, users can use the MoonBox host to provide the data resources such as storage space and bandwidth to become nodes on the Prajna Paramita Chain for getting rewards of PRMI. Like Bitcoin, the miners on the Prajna Paramita Cloud competed to dig blocks for huge rewards, whereas the mining efficiency of Prajna Paramita Cloud is proportional to the degree of storage activity, which directly provides customers with useful services. This approach has created a powerful incentive for the miners to motivate them to accumulate as much memory as possible and lease them to customers.

RPMI

Prajna Paramita Token / PRMI is based on the standard tokens issued by ERC20 with a total amount of 600 million issued. PRMI is based on the decentralized Cloud Computing and Blockchain technology. It utilizes the Smart Contracts to ensure users for sharing content of computing resources and revenues or equivalences. So as to ensure that all transactions are true, open, and transparent through the debited book records.

PRMI serves as a payment token for the Prajna Paramita Cloud platform. Users can use PRMI to pay for a series of transactional behaviors, such as storage space, content review, and sharing of bandwidth etc.

Prajna Paramita Cloud has more and more people participating in the rewards. It is getting more and more difficult to obtain, and there're more advantages to participate at the early stage. The platform encourages more individual users to join, to deliver more data nodes and bandwidth, storage, and computing resources for the shared computing ecosystem, thus enabling the entire ecosystem to maintain a good cycle.

PRMI Allocation Plan

PRMI serves as the circulation medium of Prajna Paramita Cloud platform, including transaction payment storage space, file sharing, bandwidth sharing and other settlements and recharges etc.

The total amount of PRMI issuance is 600 million. In order to maintain the healthy operation of the entire ecosystem, 70% of the coins will be used as MoonBox rewards, and the rest will be retained either in the technical teams, or remained for operation promotions, cornerstone investment and foundation etc. Briefly, the specific allocation conditions are as follows:

Rewards Generated: 70%

70% of the total circulation will be issued to users through the MoonBox rewarding mechanism.

Technical Team: 10%

10% of the total circulations shall be issued to the technical development team for their development and maintenance of the follow-up technologies for the refinement of platform ecology. It will be unlocked month by month since the tokens are put for exchange and will be unlocked by 1% per month. It will be completed in 10 months duration and completely unlocked.

Brand Promotion: 5%

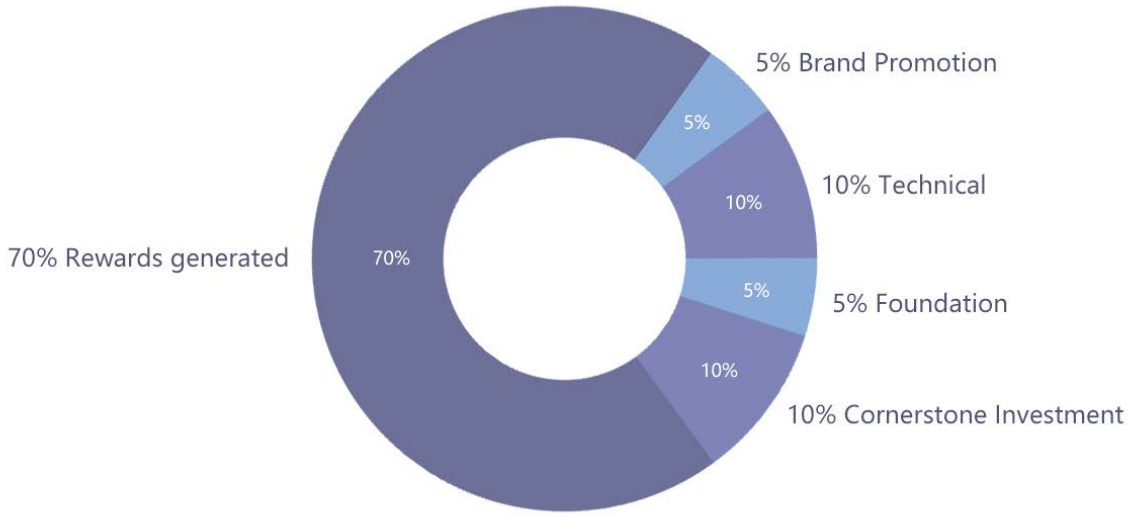
The total circulation amount is 5% as the compensation for project operation promotion costs, which are used for promotion of ecological brands both online and offline;

Cornerstone Investment: 10%

10% of the total circulation shall be distributed to partners and investment institutions. 5% of PRMI shall be unlocked after the tokens generated. The rest shall be unlocked per monthly after the month when tokens being put on line exchange. It is unlocked by 1% per month and unlocked in 5 months.

Foundation: 5%

5% of the total circulation shall be used as the reserve funds under the foundation, for the normal operation of project and the maintenance of community operations both domestically and abroad. This part shall be unlocked by 2.5% since the token generation. It is unlocked month by month since the first on-line exchange of tokens, while unlock by 0.5% every month till 5 months duration for completion.



PRMI Acquisition Method

PRMI shares ecological rewards by sharing hard disk resources of MoonBox host, the upstream bandwidth, CPU computing power, etc.Mechanism Generation

◇ Users can purchase MoonBox console, activate PRMI rewards program, and perform PRMI activities.

◇ Users can get the PRMI reward under the Blockschain Smart Contract Algorithm by contributing resources such as upstream bandwidth, shared idle hard disk storage space, CPU computing power, and hard disk read/write capability etc.

◇ Other activities announced by the official, to get the corresponding PRMI according to the rules of the event.

PRMI Reward Algorithm

Each user on the Prajna Paramita Cloud platform is a transmission node. Through Point-to-Point (P2P) data transmission, users can use the PRMI obtained by sharing idle resources as a reward. Each MoonBox will become a Terminal Server, as the Transmission Node for data storage.

Currency Algorithm

PRMI shall be issued based on the contributions of MoonBox host hardware capabilities, including the upstream bandwidth, sharable storage size, effective online time, etc. The Prajna Paramita Cloud platform shall distribute the currency generated per day to MoonBox users, according to the relevant performance weighing results through their contributions on that day.

◇ MoonBox score A = (hardware capability × (CPU factor + memory factor) + bandwidth × bandwidth affecting factor + Stored Value × Stored Value factor × (effective online time ÷ 24 hours × effective online duration factor) × day

Total currency issued per one day= Ct;

◇ Production formula: $\frac{A1}{A1+A2+A3+\cdots+An} * Ct$

Formula Analysis

◇ Hardware Capabilities:

MoonBox CPU efficiency and memory size. CPU factor weights 20, while the memory factor weighs 10 in comparison;

◇ Bandwidth:

The measured upstream bandwidth of the trusted node. In order to encourage the participation on distributed nodes, the bandwidth factor is 10 at 1-8M, turning to 5 while at 9-20M, and decreased to 1 at 21-100M, while changing to 100 at 100M; using a step-by-step algorithm (see examples as below):

◇ Storage:

The storage space measured by the trusted nodes that can be used to obtain incentive rewards is to encourage users to share more of their idle storage resources. Set the storage value to 0 while the storage space is less than 200G; while turning to 1 on condition that storage space turns to 200G-1000G, and altered to 2 if the storage value is more than 1000G; Whilst storage factor remains as 5;

◇ Read and Write:

Provided that Read/Write speed falls on range of 1MB/S-99 MB/S, then the value remains as 1; While Read/Write speed reached 100MB/S-200MB/s, the value turns to 2; Speed reaching 200MB/s, the value altered to 3, while the Writing Factor is 10;

◇ Effective Duration Factor:

The effective time constant is 1, provided that the effective online time is 24 hours for 7 consecutive days; and the valid time constant changes to 1.1, while the effective interruption often occurs during the period. The effective time constant is then recalculated from 1.

◇ Online duration:

Trusted nodes will aggregate the effective online hours of the previous day as per each day, to calculate the scores of the entire network for distributing the PRMI.

MoonBox Fractional Algorithm Example:

1. When the upstream bandwidth is 1M & storage is 100G, hard disk Read/Write speed turns to 20MB/s, while online time is 12 hours; Then the MoonBox Score = [1*(20+10)+1*10+0*5+1*10] *(12/24*1)=25

2. When the upstream bandwidth is 10M, the storage is 500G, the hard disk read/write speed is 50MB/s, and the online time is 24 hours; Then the MoonBox Score = [1*(20+10)+[8*10+(10-8)*5]]+1*5 +1*10]*(24/24*1)=135

3. When the upstream bandwidth turns to 100M & the storage increased to 1500G, hard disk read/write speed is 100MB/s, online time is 24 hours; Then the MoonBox Score = [1*(20+10)+[8*10 +(20-8)*5+(100-20)*1]+2*5+2*10]*(24/24*1)=280

4. When the upstream bandwidth is 100M, while the storage reaches 1500G, provided that the hard disk read/write speed is 100MB/s, and the online time is 24 hours which lasts for 7*24 hours; Then the MoonBox Score = [1*(20+10)+[8*10+(20-8)*5+(100-20)*1]+2*5 +2*10]*(24/24*1.1)=308

Attenuation Algorithm

◇ Decay period y:

Set the cycle of each output reduction y = 1 year (365 days)

◇ Attenuation factor d:

Each time the yield reduction is reduced by half, set d=50%

◇ Initial payment amount C:

The number of coins rewarded per unit time when starting to obtain reward coins shall be calculated based on factors as the total amount, etc. The design is C=62w/day.

The total amount of money generated by the award = PRMI production per block is halved once every 365 days, then the total amount of money generated by the award is infinitely close to around 420 million.

Application Scenario

Cloud Storage Service:

According to the actual needs of the storage size, time duration, and backup quantity, the required Cloud Storage Space can be exchanged;

Shared Cloud Computing Services:

To exchange safe and stable Cloud Computing services. To Provide ultra-large-scale distributed infrastructure and the users' cloud services with de-mediatedization and the proprietary cloud encryption technology.

Shared CDN Service:

Based on high-quality network infrastructure and Cloud Computing technology, to redeem the scalable Internet content distribution services with low cost and high-performance.

Team Introduction

Blaise Rego graduated from Nanyang Technological University in Singapore with double Bachelor's Degrees in both Computer Engineering Science and Commerce from the Polytechnic Institute. He was a mobile Java developer in 2006, and then moved to server-side Java software development and conducted the Electronic Invoices deployment on the system that has been used for two and a half years. In 2011, he returned to the mobile development domains. Since then, he has written mostly the Android C++ and Java software on independent platforms. In his daily work, he has been dealing with various other technologies as well, including JavaScript, Python, and Java SE etc.

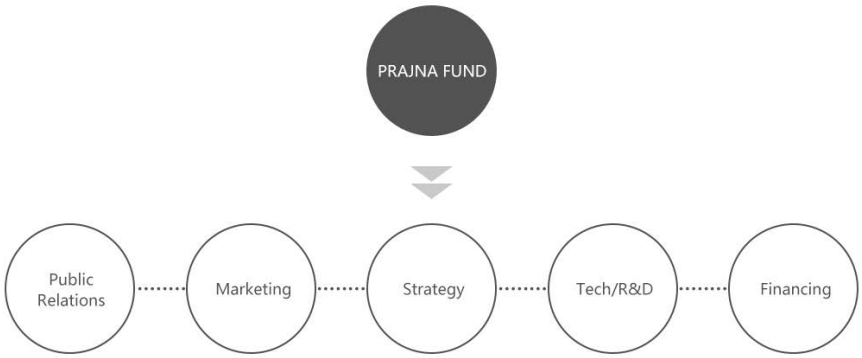
Carlos Plouviez graduated from Nanyang Technological University in Singapore with a Bachelor's Degree in computer engineering. He has in-depth research on P2P communication network security and file sharing. He is proficient in many development languages such as PHP, C#, Javascript, and Lua etc, while he started to study the Blockchain technology since 2017.

Francois Petkov is a programmer who specializes in C++ experience, focusing mainly on Ethereum and its virtual machines. Francois Petkov is the co-founder of Evmjit and has 10 years of rich experience in the design, development and deployment of software applications for large enterprises. Prior to the creation of Evmjit, Francois Petkov led the development and product management of software AG's leading host integration products.

Clarence Lam is a software engineer with over 15 years of professional experience and a Java developer mainly on server-side. While also conducted the deep researches and applications in Blockchain development, computer languages, etc.

Organizational Structure

The Prajna Foundation (hereinafter referred to as the "Foundation") is committed to the development, construction, governance, transparency advocacy and promotion work for Prajna Paramita Cloud, and has been promoting the safe and harmonious development of the Open-source Ecological Society since project initiated. The foundation will help manage general issues and privilege issues for the Open-source Community projects by developing a good governance structure for strategy implementation. The primary designing goals of the Organizational Structure of Foundation for integral governance mainly focused on the sustainability of projects for the Open-source Community, in pursuit of the effectiveness of management, and the security of funds during operation. The Foundation consists of five departments, namely the Strategy Department, Technology/R&D Development, Marketing Department, Financial Department, and Public Relations Department, as illustrated by below chart.



Statement

This White Paper is for communication purposes only, and the information or analysis contained therein does not constitute a Purchase Offer or persuasion on any kind of billing. This White Paper does not constitute and should not be construed as providing any buying or selling behaviors, nor any invitation for the purchase of any related products and virtual goods, let alone should it be considered as any form of Service Contract or commitment on contract.

Anyone involved in PRMI's purchases has behaved on basis of their own knowledge and understanding of Prajna Paramita Cloud and PRMI. This White Paper does not constitute any Prajna Team's intention to sell PRMI and does not provide any form of investment decision. Nothing contained in this White Paper can be used as a promise or statement for the future performance of Prajna Paramita Cloud, regardless of its technical specifications, parameters, performance, or functionality.

Prajna Foundation and Prajna team will not make any statements, guarantees or promises to any entity or individual. RPMI users should carefully consider and evaluate all the risks and uncertainties relating to PRMI sales (including the financial and legal risks and other uncertainties for mitigation).

This White Paper can be translated into other languages. In case of any conflicts, ambiguities or discrepancies with different translated versions, the English Version shall prevail. The White Paper will be regularly updated according to the actual needs of the ecological development of Prajna Paramita Cloud. For details, please refer to the official website for routine update records.

Prajna Paramita Chain Global Nodes Strategic Planning Layout