HOP Protocol

White Paper

Blockchain Data Center Protocol

Rev.01

Reference document only. The information herein does not constitute securities sales or solicitation in any jurisdiction.

Table of Contents

Chapter I: Project Background

1.1 Era of Web 3.0

These days the internet has grown to such a degree that it's accessible almost anywhere at any time. This has caused a large concern for its users in terms of security not just at home or work, but on the go on smartphones, tablets and the like. With more potential for abuse and misuse of user information, security is king. Modern existing Web 2.0 features struggle to keep up with the increasing demand for top of the line security, making Web 3.0 the way of the future.

In the era of Web 3.0, the decentralized feature and function of storing data in a number of different locations means there are some challenges to consider. While decentralization ultimately means more tight data security, the supervising of said platforms creates uncertainty around their prolonged ability to provide the service, thus complicating storage options on a long term scale. Nevertheless, Web 3.0 is easily placed to become the storage option of the future, allowing full autonomy of data stored in the system.

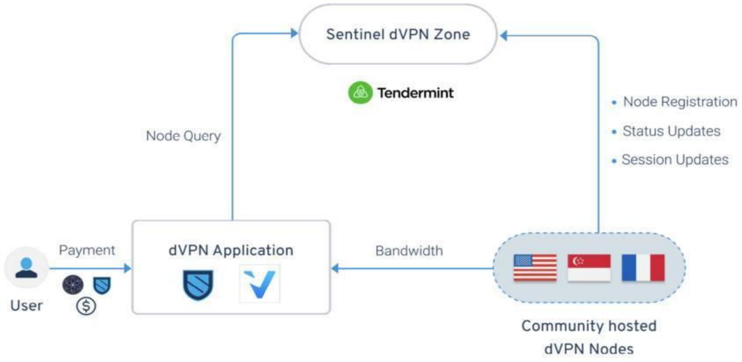
What is Web 3.0, though? If you're looking for a scientific, proper definition, you may be disappointed to find that there isn't one. In short, Web 3.0 comes after Web 2.0, which is our current internet era, in which we experience the ongoing issues caused by security breaches and theft of information through use of things like social media. Add to this, the gradual decline in the relevancy of data protection, storage and management at our disposal, means that the key issue with Web 2.0 is largely in the protection of personal data and privacy - something Web 3.0 aims to eliminate.

So, what is the alternative? Web 3.0 proposes a decentralized alternative, which is based on the peer-to-peer model. It puts forward the idea of accountability and control distribution. In essence, Web 3.0 is an architecture that cannot exist without decentralized control on a large peer-to-peer network.

The construction of Web 3.0 involves a multi-layer architecture, which aims to include aspects of underlying communication, an application layer to user layer which will feature many basic functions such as network communication, distributed computing, data storage, privacy protection and identity recognition. The realization approach of Web 3.0 does not necessarily depend entirely on blockchain technology, but starting from blockchain technology can undoubtedly build a more realistic road for the rise of Web 3.0, which is also the main reason for the emergence of a number of potential projects in the blockchain field.

Web 3.0 involves data storage, privacy protection and identity authentication. Features such as openness, decentralization, security, and other aspects all need to be realized through protocols. Compared with protocols at other levels, privacy protection protocols can play the role of technical infrastructure in building data property rights, which makes great improvement compared with functions of Web 2.0. Additionally, this takes concerted action with data security legislation actively explored by countries around the world, such as General Data Protection Regulation (GDPR) of European Union and

California Consumer Privacy Act (CCPA), thus playing a more fundamental role in the whole construction of Web 3.0.



1.2 Privacy crisis under centralization

Today is the era of data economy, and data itself has value. The search engine controls and stores the data created by users through search query, and then sends it to the data center, which in turn makes a mining analysis and sells it to enterprises. Similarly, Facebook and other social media websites build data centers around the world for use and maintenance. This also means that end users have become largely concerned and knowledgeable in the types of data that various enterprises have access to.

According to McKinsey's survey, 71% of respondents said that they would stop business contact with a company who was found to be disclosing sensitive information without permission. In response, technology companies introduced the "end-to-end encryption" (E2EE) solution, which encrypts data transmission and only allows users participating in communication to read the communication system of messages. For anyone eavesdropping on the conversation, even the service company, they cannot access the encryption key needed to decrypt the information.

E2EE is an important tool to protect some types of data transmission but it is only a partial solution. E2EE for example has no effect on protecting metadata, or who sends data to whom when, where and how often. At the same time, E2EE is not enough because it still has man-in-the-middle attacks and backdoor programs. There have been a number of attacks accessing the data of thousands of people in recent years not just on social media platforms like the WhatsApp E2EE breach, but on various banks as well. Using the decentralized Web 3.0 would eliminate any such breaches of security and provide a much safer environment for potentially sensitive information.

At present, e-mail does not use any E2EE, so it is easy to be deceived in the likes of a phishing attack. The result is continued expansion of criminal networks, working to deceive others or install malware or ransomware onto computers through clever emails disguised to look authentic and legitimate.

1.3 HOP project objectives

1.3.1 Construction of global service infrastructure

HOP is an open incentive and decentralized hybrid network which can realize point-to-point data exchange to protect privacy. It is private, decentralized and economically sustainable.

At HOP, we hope to build a network-level service infrastructure that integrates data flow, data storage and metadata to protect privacy. This is our true vision, and we have a comprehensive plan to bring out vision to life.

Our vision is based on the following two main aspects:

Firstly, we provide technical solutions for network-level privacy. With existing technologies and some cutting-edge innovations, we can create a decentralized incentive network operation and maintenance environment based on flow, storage and metadata, all of which is maintained by users. The users can then communicate, share and maintain data in an untraceable way.

Secondly, we put forward a governance plan. As time goes on, we build, maintain, operate and improve the network so as to ensure that the network is financially self-sustaining and completely controlled and managed by the users.

We comply with laws and regulations and protect the rights of network members. We give members, not the project team or even the board of directors, the executive control power.

HOP believes that we need to work out an overall solution if we want to ensure privacy and security. Through the global network security incidents, we find that the problem of privacy leakage is sometimes at the flow side and sometimes the data storage side. Even vulnerabilities in browser, docker and virtual machine can often bring challenges to our privacy. Therefore, we should adopt an integrated scheme to protect privacy, instead of just solving the problem in one aspect. Additionally, because decentralized blockchains have a value system, the work between blockchains is more efficient allowing for various costs associated, such as gas, to be reduced.

HOP Protocol provides network-level and metadata privacy for each data exchange. The hybrid network protects the identity of both the sender and the recipient entity via route data of multiple intermediate relay hops for mixed flow and safe storage of data. As economic incentives are provided, the global privacy network can be deployed and operated on an enormous, sustainable scale without affecting privacy. Using P2P (end-to-end) network transmission and blockchain technology, the HOP team establishes a blockchain micropayment protocol based on the blockchain transmission encryption protocol between P2P network bandwidth contributors and bandwidth users. It then merges it into a flow mining and mining pool. The whole protocol is built on the mainnet and is given micropayment and mining functions. In addition, HOP supports the flow mining of ERC20 in any currency. Up to now, HOP is the only protocol in the world that combines the above functions and is officially used. Its birth provides an absolutely secure access terminal node for any service related to flow bandwidth.

Chapter II Implementation of HOP Protocol Core Technology

2.1 Overall architecture of HOP protocol

Data packet consumer & product		
Data packet market		
Data packet-wallet	Ethereum balance	
	Token balance	
	Data packet usage & balance	
Micropayment protocol	Payment channel	.Micropayment .P2P data encryption
	Data channel	.Data packet mining
Blockchain	Smart contract	
	Transfer	

The architecture design of HOP supports both public blockchain as well as alliance blockchain and provides a unified privacy protection protocol overview for different application scenarios. It has a two-layer network of communication storage and incentive mechanisms.

HOP is a private network protocol that can communicate and transmit messages securely. This is defined by the payment layer, which is distributed ledger technology (DLT) or blockchain infrastructure, and can open the payment channel on behalf of the HOP nodes running the HOP network.

In its first implementation, HOP currently relies on Ethereum blockchain as its payment layer. Using Ethereum smart contract, we open the payment channel on behalf of HOP nodes forwarding messages. The message sender then attaches HOP tokens to its messages. Once successfully delivered, these tokens will be paid to the HOP node relaying messages.

To realize this, the HOP node implements a connector interface, which communicates with the Ethereum blockchain using its popular Web library web3js. These interfaces allow HOP nodes to monitor, approve, sign and verify when to transmit messages, so as to close the status channel and receive the HOP token they obtained. Each HOP node verifies each other, avoiding foul and rewarding honest relay officers only.

Although the first instantiation of HOP network is in Ethereum blockchain, HOP is an independent of blockchain, meaning that HOP nodes can finally realize different payment channels in different blockchains, adding to its appeal as both universal as well as secure.

Developments currently in progress indicate that in the near future, HOP will be able to realize Polkadot's payment gateway.

A. Background

Messages shall be transmitted in a secure manner. The meaning of security seems to be intuitive. However, upon quick in-depth study, secure communication is a complex problem:

Secure communication shall prevent unauthorized parties from learning the contents of messages. This security objective is called confidentiality, which can be achieved by AES and other reasonable encryption schemes.

Secure communication allows the sending of messages in such a way that messages are not changed, or at least the designated receiver can observe any operation on such messages. The attribute is called integrity and can be achieved by using a suitable scheme that generates HMAC and other message verification codes.

The two schemes (i.e., confidentiality and integrity) produce a structure that allows the sender to hide the content of the message and make the integrity of the message verifiable.

However, this construction does not hide the fact that a specific sender and receiver have exchanged messages. Unfortunately, this construction leaks an upper limit that shows how much communication has occurred. Therefore, possible opponents may also distinguish short conversations from longer conversations. If the attacker can also observe the action after receiving the message, they can infer the content of the encrypted data observed, without destroying the encryption scheme. This indicates that confidentiality and integrity are insufficient in some cases, so it is also necessary to protect metadata.

B. Anonymous service

In order to hide the communicator (i.e., communication metadata), the sender and the receiver need other parties to help them hide the metadata. Without these additional participants, any communication between the sender and the receiver can be checked. As described above, it is not affected by timing attacks, and is independent of the encryption or verification scheme used in the channel.

In order to protect themselves, the sender and the receiver need to rely on anonymous service providers. In most (if not all) cases, these anonymous service providers will generate economic costs. These costs include not only the procurement cost of necessary hardware, but also electricity or bandwidth costs and other recurrent costs. In addition, handling complaints of abuse may also generate legal costs. These third parties can choose to provide the service free of charge and incur any such costs on their own, but with economic incentive provided, it allows for widespread monetary gain for those parties who offer anonymous services.

C. Economic incentives

If there is no motivation to provide anonymous services, people who use these services need to rely on the altruistic nature of the providers if they are to do so for minimal costs. Such providers do exist, but it will be naive to rely solely on the proviso that they are large enough to support an extensive and reliable network, especially if those parties are seeking a network that can run large applications.

It is necessary to encourage participation by compensating providers who provide anonymous services. The costs involved in running the networks many users seek could essentially price many potential providers out of the market. Only by economic incentives can we have a reliable and self-sustaining communication network that many users will be seeking.

The software and hardware implementation of HOP Protocol can act as HOP nodes, and then create a decentralized network called the HOP network. Users of the HOP network can use different HOP nodes to relay messages through multiple "hops". In order to exchange HOP nodes under stable operation, these intermediate nodes get payment by using the blockchain payment channel, with the possibility of obtaining a digital token (such as a HOP Token) as payment for their services.

Messages relayed in the HOP network are in a secure data packet format to avoid leaking any data about their contents. Therefore, both the sender and the receiver do not have to trust the HOP nodes in the network. As a result, HOP nodes cannot check the data that has been relayed. But after successfully relaying messages, they will be rewarded in digital currency, such as the HOP token.

D. Hierarchical architecture

The HOP Protocol consists of two main layers: message delivery/data storage layer, along with the payment delivery layer.

E. Message transmission

Messages transmitted using HOP Protocols are embedded in the SPHINX data packet format, which can prove that the relationship between the sender and the receiver is hidden. These messages are transmitted through the network layer, created through peer-to-peer connections between HOP nodes. In the background, HOP Protocol realizes the combination of libp2p and WebRTC to bypass NAT. This allows HOP nodes to become intermediate nodes that relay messages and obtain HOP tokens.

F. Payment layer

The payment layer settles the balance of the HOP Node operator through the off-chain payment channel. In order to deal with transactions, HOP node operators need to obtain encrypted assets. After successful data relay, they will get a ticket, which may get HOP tokens. Then, when the payment channel is closed, these tokens can be settled and used as a payment method for requesting services from other HOP nodes in the network.

G. Mixed flow

HOP mainnet will be an incentive decentralized hybrid network. In order to make the hybrid network truly private and secure, we need to use the so-called 'mixed flow'. This is arbitrary data transmitted through the network, to cover up the real data sent between users. As this layer of extra data constantly moves through the network, people outside the network cannot extract any metadata about who is using the network and how much data is sent through.

The HOP Protocol team is committed to providing friendly interfaces for blockchain technology platforms and DAPP applications. By applying such interfaces, users can build and use various applications conveniently and quickly. It will have design optimization derived from the following attributes:

1. Accessibility. Decentralized applications shall be as easy to use as current Internet applications In addition, the development of decentralized applications shall be as easy as the current cloud development.

2. Expandability. Decentralized applications shall support Internet-level users, that is, hundreds of millions to billions of users. To achieve this, the network (including blockchain) must be expanded to incorporate these numbers and applications.

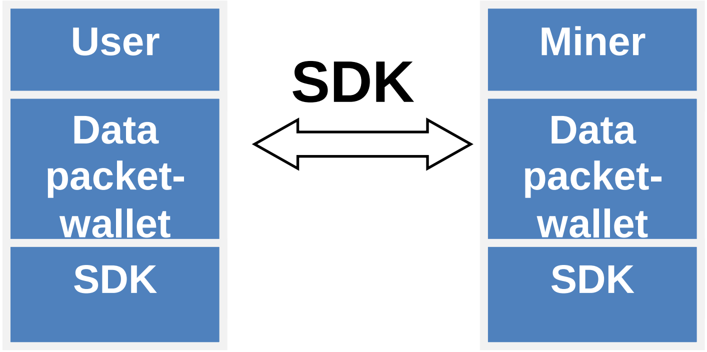
3. User control. Applications using decentralized computing shall be controlled by users by default. Users shall provide their own computing and storage resources, instead of relying on the servers operated by applications.

With these design objectives, HOP has made its own design choices, which have distinguished it from other decentralized computing schemes of "heavy" blockchain and "world computer" design philosophy.

The view to minimizing the logic and state of blockchain layer should be considered. In order to get the expandability, HOP Protocol minimizes the logic and data of application in our "light" blockchain layer. Recording application logic and storage via blockchain is inherently slower than the "off-chain" method. It is necessary to synchronize and verify the status in the whole network and among devices, which shows that this operation has great limitations. The limitation factors are the underlying global connectivity bandwidth and the available memory on typical network nodes.

The change in local and global states is another point. The HOP Protocol platform uses the full-stack method to ensure that applications built on HOP Protocol are expandable: The interaction with applications changes local state as much as possible. Because of this, our storage system and authentication protocol are the basic components of our platform. It enables applications to interact with users' private data storage and complete user authentication without initiating a blockchain transaction. The HOP Protocol blockchain is only used to coordinate the transformation of global state in a consistent way in a decentralized environment (for example, registering a globally unique user name).

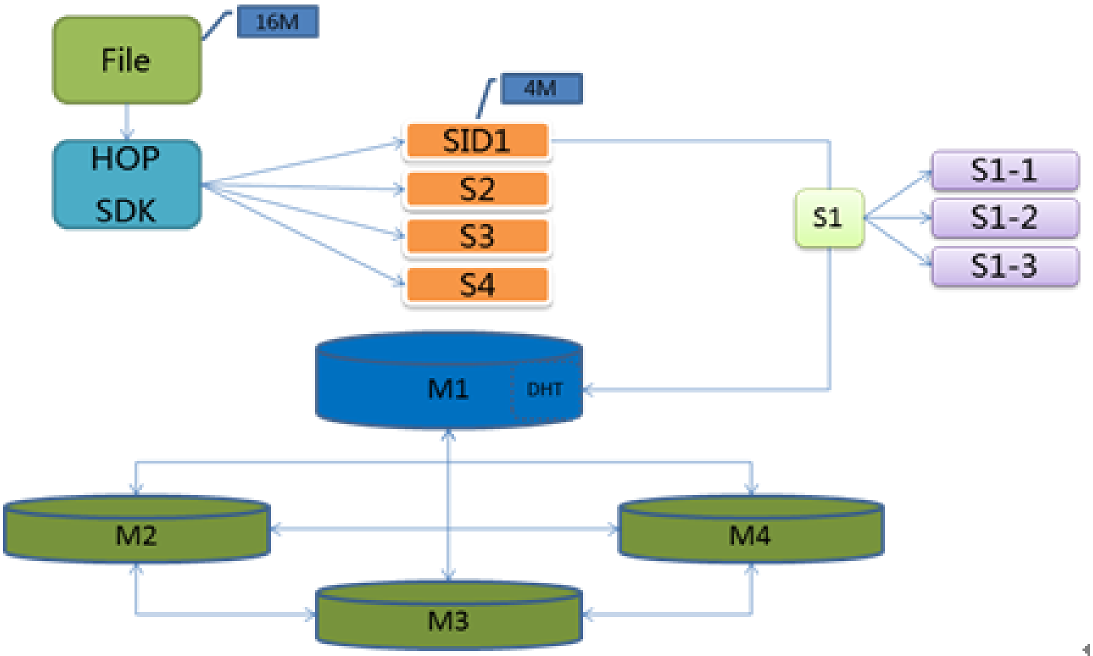
Another attribute will be full-stack SDK for developers. HOP Protocol provides a full-stack method and default options for all layers needed to develop decentralized applications. The developer, SDK, separates the complexity of blockchain from other development technologies; application developers can easily build their applications using HOP Protocol. Different levels of technology stack are modular, and other technologies can be used as needed.



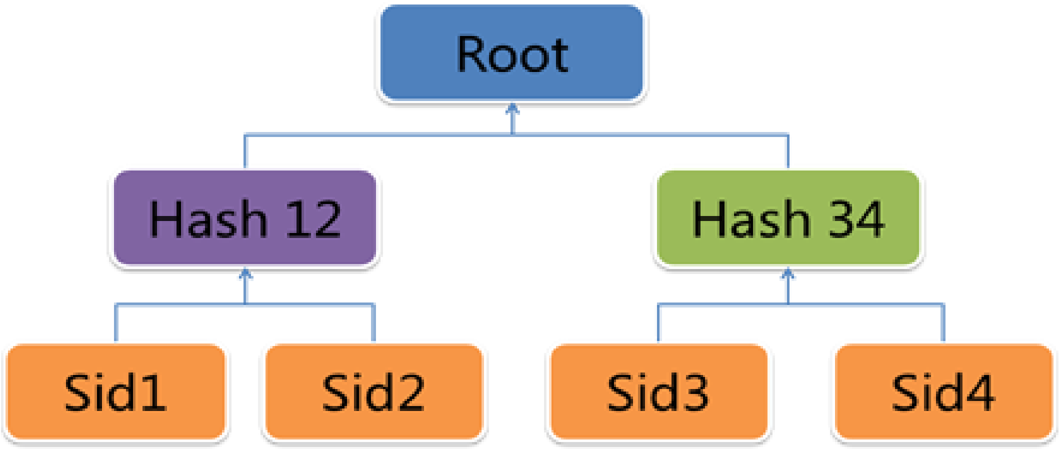
Flow protocols can adapt to a variety of scenarios.

2.2 Establishment of storage mechanism through decentralized protocol for HOP

HOP takes distributed flow sharing as the breakthrough point to constitute a huge flow proxy network, which originates from the traditional Internet architecture and centralized storage equipment. Under the existing Internet infrastructure, there are 2 types of network data: One is real-time interactive data, such as voice conference, live video broadcast and games, whereas the other is non-interactive data, such as video on demand, website browsing and cloud disk data. For the first kind of data, HOP provides encryption, desensitization and anti-tracking functions for network data through the flow proxy network. For the second kind of flow data, the HOP Protocol will rely on existing network proxy nodes to create a distributed file storage system. The basic principle of the system is as follows:



For any video data, file and executable code, HOP will provide a complete client program, broadcast the data to HOP network in fragments, and the storage nodes in the network will store such fragments in a redundant form for visitors to use.



For a file F, its size is S bytes. According to a certain fragmentation rule, if the file is fragmented according to the size of P bytes (S/P+1), fragments will be generated. For any fragmentation object Si, its data is less than or equal to P, and HASH operation is performed on the data to obtain the unique representation, namely, Sid = HASH (Si); then duplicate X redundant copies of Si and submit the data to HOP network; where X represents the system's fragmentation redundancy of data, and X is 3 by default.

Before submitting it to the HOP network, it is necessary to perform a Merkle tree operation of file structure for all fragments of file F. The Sid of every 2 fragments is taken as the leaf of Merkel tree, and the final calculation result is the root of the Merkel tree. SDK then returns the root to the caller of SDK, and returns the structure of the Merkel tree to the caller as a file information expression table. The caller takes the root as the file name and the Merkel tree structure topology information as the file description. This data result can be used as a part of the Linux file system and can be mounted under the disk letter of the operating system.

Data redundancy fragments can be submitted to different nodes of different HOP networks, or same nodes which are not restricted by the protocol. After receiving data fragments, HOP network node Mi calculates the data distance Di = Sid XOR MAi between the data address MAi of this node and the fragment. Through its own DHT table, ask whether there is a HOP node address and whether there is node Mj, so that Dj is less than Di. If it exists, the data fragment is passed to the node Mj, and the node Mi stores the data in its own temporary data storage area. As for the expired market of the temporary data, Esimi = 1/Di * Eg, Eg is a global parameter indicating the expiration time of temporary data of the whole network. That is, the larger the data Distance Di, the shorter the time for nodes to cache data. If no node Mj exists, making Dj is less than Di, the node Mi stores the allocation in the local permanent storage area, and searches for X-1 storage nodes Dk with a distance of Di-1. In the case of X-1 = 0, the system storage ends.

Through the distributed storage capability of HOP, the flow distribution capability of the HOP network can be greatly improved and the usage scenarios of HOP network can be enriched. For non-interactive data, the storage capacity of the HOP network can greatly improve the data access speed and shorten the data transmission path. For example, if you hit film and television play, some nodes of the HOP network will obtain data through the traditional Internet. After this, they can store the video data fragments in the temporary storage area. When the same data request occurs, the HOP Protocol client does not need to reload the data from the traditional Internet, and the HOP mining rig node will directly give the data fragments, thus creating a relay of data that is lightning fast.

For some contributors of similar short videos, they can upload data to the HOP network through the SDK of HOP and the nodes of HOP network can safely and reliably store the data and provide particulars of the response. After contributing the file name and description information to other users, video contributors can quickly access the data through the HOP network and get digital currency in return. The network nodes will also get the corresponding digital currency through the micropayment technology of HOP. (discussed in Section 2.4).

2.3 HOP Protocol security encryption protocol

As mentioned previously, network security and the risks of user privacy have always attracted our attention. HOP security encryption protocol adopts peer-to-peer (P2P) network underlying layer. From the technical point of view, blockchain technology is P2P+consensus, mechanism+cryptography. Essentially, blockchain technology is a P2P network architecture, which ensures data security through cryptography and data consistency through a consensus algorithm. With the distributed P2P network along with blockchain, there is basically no single point of failure. Even if nodes advance and retreat frequently, they will not affect the system as a whole.

We know that there are many blockchain projects, but we can divide these contents into three categories: public blockchain, private blockchain and alliance blockchain. The public blockchain is completely open, so it determines that it will not adopt P2P encryption in the network. For the other two (especially the alliance blockchain), their nodes cooperate with each other but do not fully trust, making the P2P network particularly important.

The P2P network itself has many advantages, with its application in blockchain as follows:

★ Decentralization

The resources and services of blockchain are distributed on all participating nodes, and the consistency of the blockchain network is maintained through a consensus mechanism without the existence of a central system.

★ Expandability

Blockchain nodes can join and quit freely and the network system can expand freely according to nodes.

★ Robustness

The blockchain network has no central nodes, so there are no targets of attack. Participating nodes are distributed in the network, but the damage of some nodes has no impact on the blockchain system. (We know that many protocols are handled by CA, which has become the target of attack in recent years). The benefit is that the blockchain does not have the mechanism of CA, so risks are avoided.)

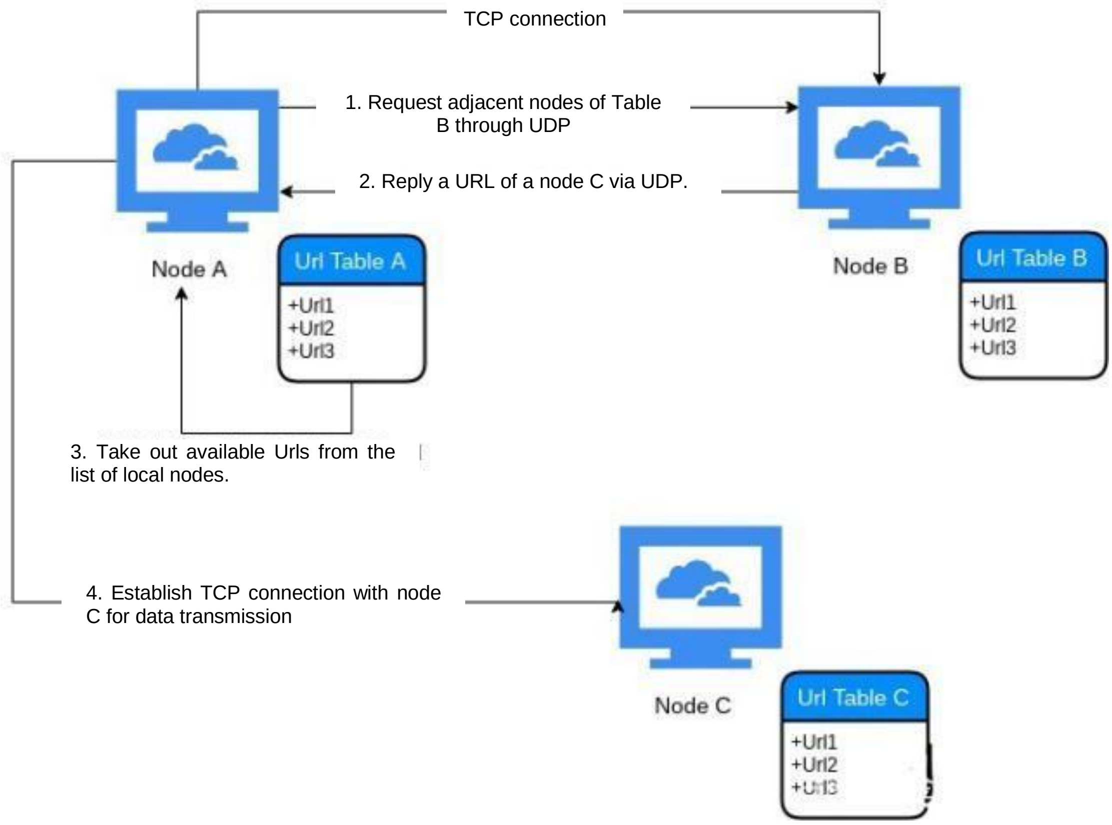
★ Privacy protection

Block information adopts a broadcast mechanism, which cannot locate the initial broadcast node. This prevents users' communication from being monitored and protects users' privacy.

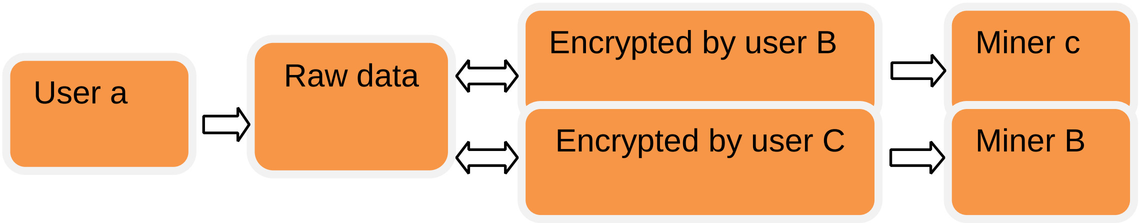
★ Load balancing

Blockchain avoids resource loading and network congestion by limiting the number of node connections and other configurations.

Based on the above characteristics, HOP Protocol adopts fully distributed P2P nodes to join and quit freely; there are no central nodes, there are no structured and unified standards for node addresses, the whole network structure is a random graph structure, and there is no fixed network structure diagram. However, complete freedom means that new nodes cannot know the information of P2P network nodes, so they cannot join the network. As a fully distributed P2P network is freer, there is a problem with node management. The frequent joining and quitting of nodes makes the whole network structure unstable and a large number of broadcast messages not only wastes resources, but even blocks the network.


TCP connection
1. Request adjacent nodes of Table B through UDP
2. Reply a URL of a node C via UDP.
Node A
Url Table A
+Url1
+Url2
+Url3
Node B
Url Table B
+Url1
+Url2
+Url3
3. Take out available Urls from the list of local nodes.
4. Establish TCP connection with node C for data transmission
Node C
Url Table C
+Url1
+Url2
+Url3

To solve the privacy problem of blockchain, the solution of the HOP Protocol project is to build the HOP encryption protocol based on the P2P underlying layer. In the process of value transmission, HOP hardware provides a stable computing system through Starlink and the flow equipment. It then outputs more compliant computing power value and establishes micropayment channels that can circulate in two directions for different networks. Digital assets can be transmitted across nodes, reducing the load of related parent blockchains. HOP Protocol encrypts the data packets in the network many times, and the network intermediate layer value can open the corresponding encryption layer. This mainly displays the transmission node and routing information of this packet, thus hiding detailed information such as transaction and file transmission.



P2P data encryption

2.4 Micropayment based on HOP

HOP Protocol payments will take advantage of the distributed characteristics of blockchain and use multiple nodes around the world to better ensure its integrity and flexibility.

HOP Protocol payments will use secure encryption protocols and lightning network in its payment processing engine. This will realize transactions without trust, and eliminate the need for traditional methods such as third-party notarization and alliance authentication. According to needs, only the final balance will enter the blockchain mainnet to reflect the end of the payment channel. HOP payment users can pay for services from their HOP wallets to services connected through SDK.

You will be able to access payments through HOP Protocol Wallet, which will appear as a browser plug-in, similar to MetaMask. Therefore, smoother user experiences can be realized through seamless integration among HOP payment services, websites supporting HOP Protocol SDK payments and users' HOP Protocol Wallet. This wallet will pay through its electronic wallet function on the merchant platform that supports HOP payment. In traditional cross-border payment, there are often risks such as high transfer fees, long settlement period, slow arrival, limited transfer amount and fund freezing, which often bring unnecessary losses to the operation of enterprise users. It is difficult to make breakthroughs for cross-border payment in the traditional financial system, while the friction-free, real-time and efficient decentralized payment network provided by blockchain is an effective tool to solve the pain points of cross-border payment issues.

The HOP Protocol Wallet will be open-source in the future, allowing for independent auditing. This shows that the application is guaranteed in terms of quality, privacy and security, and consumers can use it securely.

The next generation Internet Web 3.0 has been conceived as a full-featured and user-friendly website, in which our identity and data are our own. Because the distributed blockchain technology is adopted, it is not protected by any central organization. We believe that no blockchain can finish all the work; HOP itself provides 3 blockchains: flow, storage and metadata. They are independent of each other, but they are still connected with each other in work, so we introduced the blockchain bridge.

A blockchain bridge is a connection that allows transmitting tokens and/or arbitrary data from one blockchain network to another. The two blockchains can have different protocols, communities and governance models, but the network bridge provides a compatible way to interoperate safely between the two parties. The HOP payment agreement is our blockchain bridge. Payment protocol is a so-called blockchain bridge of distrust, which means that users don't have to put trust in a single entity or authority, but put trust in the bridge of mathematical truth built in the code. The untrusted interaction is implemented by the technology (and/or incentive mechanism) behind the system, instead of commitment or legal agreement. It is designed as an infrastructure, which can realize the expandability, interoperability and security required by multiple blockchains in the future, thus allowing mutual interaction and communication of various blockchains within the ecosystem. It also allows interoperation of parallel blockchains and external networks (such as Bitcoin or Ethereum) through bridges.

2.5 Distributed computing power

In the HOP public blockchain network, mining rig nodes have rich capabilities and roles, which can be configured according to the characteristics of different equipment. The roles of the mining rig include a consensus mechanism, generating distributed ledger, forwarding flow, contributing storage content, and collecting computing power. Among them, collecting computing power is the most difficult problem in the field of blockchain technology.

The HOP Protocol is based on the application of the Byzantine fault tolerance algorithm in the field of consensus. This develops and designs the mechanism of collecting computing power. Each node of the HOP public blockchain will be randomly assigned with an execution code, which is also randomly assigned to other nodes with computing power collection functions. The goal is to complete the execution of the code within a specific time and submit the results.

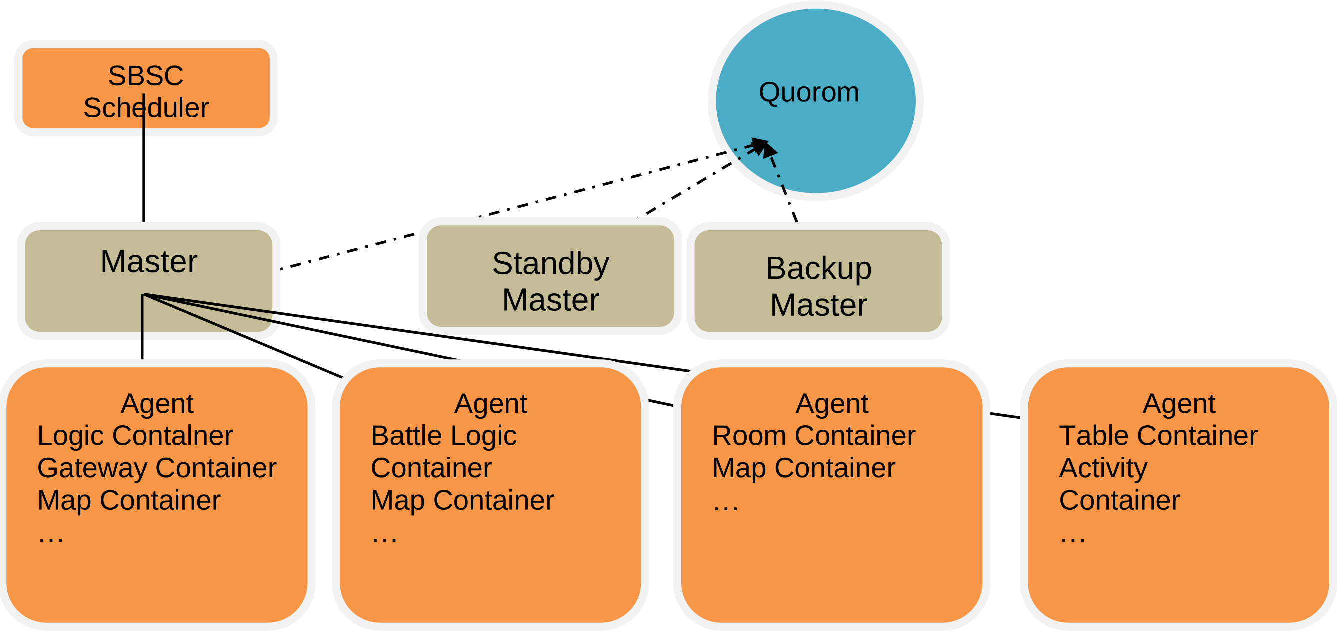
A fixed number of nodes with computing power function are directed to an assignment, S, by a random algorithm. For a computing task, P, it will be divided into N fragments by the submitter. Each fragment task is P. For the number of nodes in an allocation, Sn, it is generally set to n= Sn / 4a (where A is a positive integer, indicating the requirement of computing power accuracy. The default value is 1. The larger A is, the higher the computing accuracy and the more reliable the computing result). After the task is fragmented, it will be assigned to HOP public blockchain nodes with storage functions enabled according to the storage mechanism described in 2.2.

For nodes with computing power collection enabled, HOP public blockchain nodes receive the same computing task fragments, with G being a group. Within a specific time, T, all nodes in G shall give calculation results and give each other an intermediate calculation. They collect and synchronize the intermediate results through the Byzantine fault tolerance mechanism to ensure the calculation errors of non-malicious computing nodes under special circumstances. When T ends, all nodes in group G give the results to the computing power submission nodes respectively. The submission node verifies the validity of the result of task assignment, P, through the Byzantine fault tolerance algorithm again, and penalizes the nodes that fail in calculation and rewards the nodes that succeed.

In theory, the execution time of task P, is NT. Each fragment calculates the number 4A of nodes in group G. When Sn is larger than 1,024 nodes, and the intermediate result check interval T is more than 30 s, the distributed computing power of the HOP public blockchain is more bandwidth-saving, power-saving and faster than traditional cloud computing for a sufficiently large computational task.

The disadvantage of distributed computing power of the HOP public blockchain is that it can only perform large tasks that can be split. Fortunately, with the development of technology, the coupling of large-scale data is getting lower and lower. With more and more data needing to be cleaned and initially processed before the next coupling operation, the application range of the HOP public blockchain will be wider and wider.

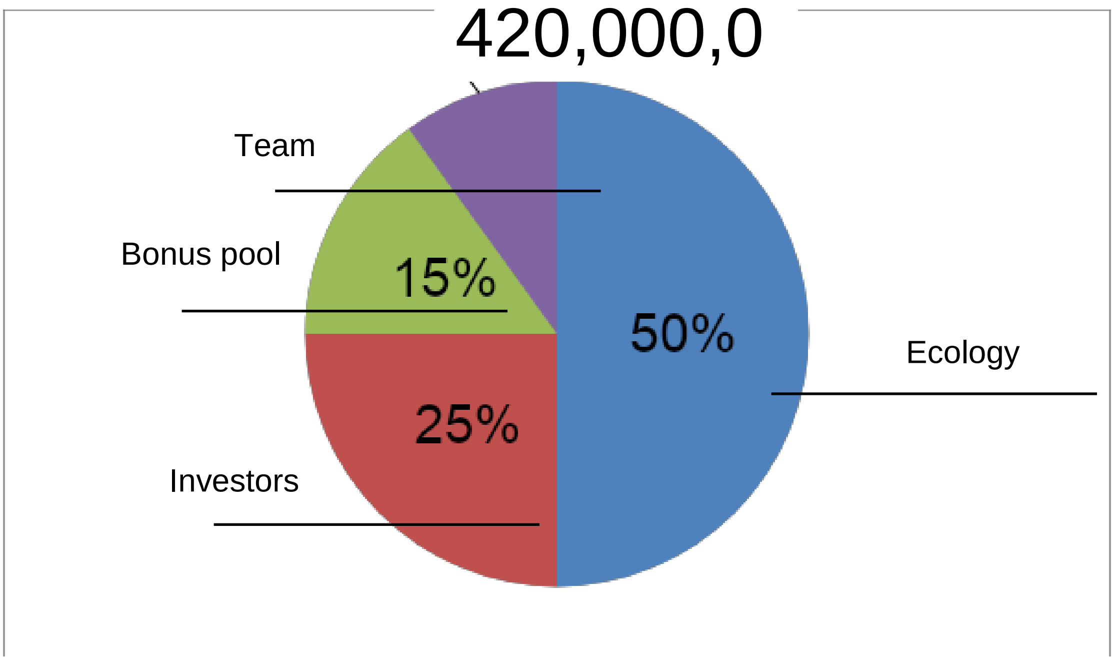
In this example, the artificial intelligence learning and computing of autonomous driving need to consume huge computing power. The raw data scanned by cameras and radar have extremely low coupling data, which will consume huge storage and computing costs through cloud computing. The distributed computing power and distributed storage of the HOP public blockchain can greatly collect low-cost storage and computing nodes. Similarly, the early processing of various large-scale computing tasks can be sent and reliable results through the HOP public blockchain can be collected.



Chapter III HOP Protocol Token Economy

3.1 Allocation principle of tokens

The amount of tokens issued by the protocol is 420 million. HOP is a negotiable and ecological token, which is used in a number of ways in the HOP Protocol platform ecosystem. The founding team thinks that HOP, as the first project with huge market scale and significant application value, is a digital commodity with real service exchange value. The flow value required by each newly generated digital commodity will increase with the difficulty of issuance. The earlier you hold it, the more likely you are to redeem more services.



The technical team and the investor will lift the ban in proportion to the number of miners. We regard the technical team, ecological fund, miner and supernode as a community of interests. The whole community then benefits from the participation of the miners.

3.2 Flow mining platform

The HOP Protocol flow mining platform mainly uses and consumes bandwidth flow, but can also be an independent APP. Its hardware only needs to run the HOP Protocol terminal software, which includes but is not limited to: smart phones, personal computers, intelligent hardware, routers, Pads, servers, IDC computer rooms, AWS, Azure, Alibaba Cloud and other terminals, all of which can become nodes of the HOP network. A large number of nodes will play two important roles in the future. Firstly, they will share flow, storage and computing power resources to provide the request with network acceleration, data storage and cloud computing services. Secondly, it will ensure data credibility and immutability based on distributed ledger maintenance of the blockchain.

The founding team of the HOP Protocol has fully mastered the core technologies including distributed CDN, intelligent scheduling, dynamic deployment and dynamic defense. It has implemented a set of efficient scheduling schemes by leveraging the accumulation of P2P cloud computing for many years in order to grade users according to service quality, and rationally allocate computing tasks. The mining conversion rate of users is as high as 99%. The request sharing CDN platform has strong purchasing power as well. Video on demand, on-line live broadcast, game downloading, intelligent hardware, mobile applications and other popular Internet fields are our target user groups, who are eager to get cheap bandwidth and agile bandwidth deployment support.

3.3 HOP Protocol node

HOP Protocol edge flow is one of the sub-plans of the whole ecology, which aims to create economic value by using the bandwidth of edge computing. Differing from other services, edge nodes need a scheduling, stable and reliable environment. Therefore, we have added a corresponding pledge mode in the design, to make the whole network more stable and reliable. There will be certain punishment measures for unstable users.

1. Home node

To encourage participation, the HOP Protocol lowers the threshold of mining. Node sharers of ordinary personal computers can conduct mining without spending money in adding goods and pledge. Mining can be divided into intelligent and full-speed mining along with other modes, allowing multiple purposes of one computer, which meets various personal needs, and can also be exchanged for HOP. Ordinary nodes mainly collect idle bandwidth resources from ordinary users and deliver them to customers who have no strict requirements on bandwidth quality. They can also be transplanted to network terminal devices such as home routers, set top boxes, Pads and mobile phones, and has strong cross-platform expansion usability.

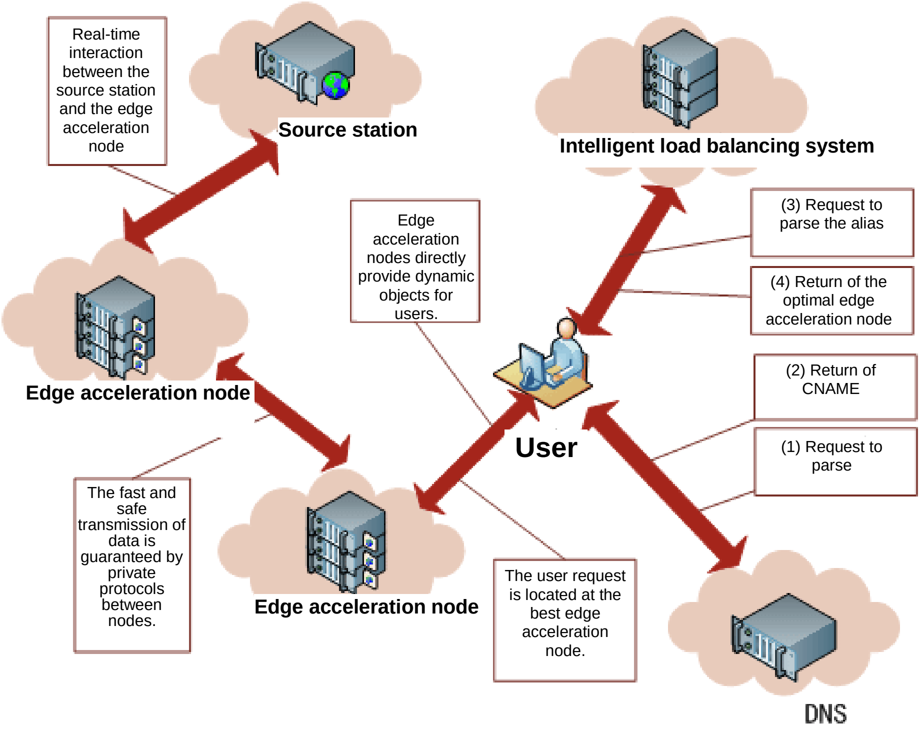
2. Supernode

Idle bandwidth of a single home is not enough to support a stable edge distributed network. Because home bandwidth is unstable, with minimal capacity, we introduced the IDC supernode plan, aimed at introducing some IDCs. IDC has a stable network environment, and combined with BGP multi-line access, uninterruptible power supply (UPS) and professional operation and maintenance management, it brings us a stable network environment.

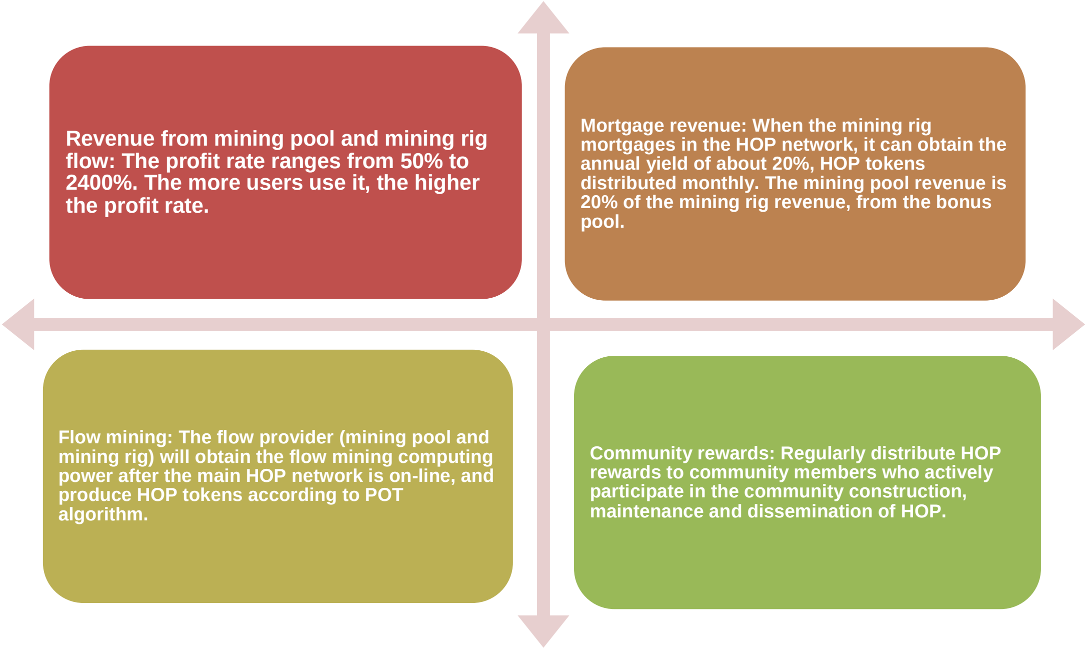
	Network	Public network IP	Capacity	Stability	24 h operation and maintenance	Income coefficient
IDC	BGP multi-line	Yes	Gb	Special	Yes	2
General	Home bandwidth	No	Mb	Multi-purpose	No	1

Environmental comparison

The IDC participation plan is to ensure the effective implementation of the HOP Protocol edge node plan and ensure network stability. In the design, we consider the plan of joining and quitting nodes, and the revenue plan also designs bonus revenue for IDC nodes.


Real-time interaction between the source station and the edge acceleration node
Source station
Intelligent load balancing system
Edge acceleration nodes directly provide dynamic objects for users.
(3) Request to parse the alias
(4) Return of the optimal edge acceleration node
Edge acceleration node
(2) Return of CNAME
User
(1) Request to parse
The fast and safe transmission of data is guaranteed by private protocols between nodes.
Edge acceleration node
The user request is located at the best edge acceleration node.
DNS

3.4 The Revenue of HOP



Revenue from mining pool and mining rig flow: The profit rate ranges from 50% to 2400%. The more users use it, the higher the profit rate.

Mortgage revenue: When the mining rig mortgages in the HOP network, it can obtain the annual yield of about 20%, HOP tokens distributed monthly. The mining pool revenue is 20% of the mining rig revenue, from the bonus pool.

Flow mining: The flow provider (mining pool and mining rig) will obtain the flow mining computing power after the main HOP network is on-line, and produce HOP tokens according to POT algorithm.

Community rewards: Regularly distribute HOP rewards to community members who actively participate in the community construction, maintenance and dissemination of HOP.

HOP Business Model

1. Redemption of storage space

The user can redeem personalized cloud storage services. Only oneself can get access to complete files through private keys designed to protect privacy. Simultaneously, they would provide large scale storage solutions for a variety of enterprises.

2. Redemption of CDN acceleration services

HOP token holders can use HOP as fuel for functions such as downloading, uploading and file acceleration in the network acceleration task system.

3. Secondary market benefits

With the increase of demand and supply, both the difficulty and the value of HOP increase rapidly. The price expectation of the secondary trading market also rises with the fluctuation of market demand, so as to achieve profits of HOP holders.

4. Huge demand

The storage market for files, videos and other information and data is huge, with broad development space and market prospect. All HOP holders, contributors and demanders will gain benefits.

5. Participation in the community and getting rewards

As for all supporters, as long as they actively participate in community construction, maintenance and dissemination of HOP, their contribution will be evaluated at each business stage and HOP rewards will be issued to supporters who have made great contributions.

	Expenditure	Income	Profit	Profit rate
Server cost	200 USD/Year	/	/	/
10 users	+0	300 USD	100 USD	50%
20 users	+0	600 USD	400 USD	200%
50 users	+200 USD	1,500 USD	1,100 USD	275%
100 users	+200 USD	3,000 USD	2,600 USD	650%
1,000 users	+1000 USD	30,000 USD	28,800 USD	2400%

Flow service revenue of HOP

Chapter IV Future Business Scenarios of HOP Protocol

4.1 Starlink and Space Internet

Starlink is a global high-speed Internet access service launched by SpaceX, a space service company, with a view to providing internet services through low Earth orbit satellite groups. This is a space high-speed Internet plan announced by Musk in 2015. By deploying 42,000 satellites in low Earth orbit, high-speed Internet services will be provided for everyone on earth.

The "star" in the "Starlink" is a satellite. The name comes from the star appearance that satellites can have when the number of artificial satellites reaches a certain level.

The **"link" in the "Starlink"** means that it is necessary to realize the interconnection between satellites to provide wireless microwave access to each, but also to realize the function of routing and forwarding data in space.

Low Earth orbit: This means that the orbit of the satellite in the "Starlink" plan is not the same type as traditional satellites, but is in fact much lower.

Satellite groups: This means that the "Starlink" plan will need a large number of satellites in order to function correctly. A giant satellite group consisting of 12,000 satellites is scheduled to be deployed in orbit, bringing this plan one step closer to realisation.

Global coverage: Different from 4G/5G access provided by operators in different countries, "Starlink" is a global high-speed microwave wireless access provided by a single equipment supplier.

High speed: It means that, unlike traditional satellite communication, "Starlink" plan can provide 50M-100M wireless access, which far exceeds the current level of satellite communication and reaches the level of 4GLTE transmission rate.

Internet: Traditional satellite communication mainly provides voice services and some data services. The "Starlink" plan provides video services at the current mobile Internet level.

Remote: According to information recently published by the UN, roughly 57% of the world currently do not have access to the internet, largely due to infrastructure in many places. “Starlink” aims to provide an easy access option for internet users to get online, regardless of location.

In brief, "Starlink" expands the mobile Internet from the ground to space, which is similar to, and even greater than 6G. "Starlink" can completely replace the current cellular mobile communication network. As a new type of wireless access and mobile network covering the whole world, it will subvert the traditional network operators and equipment networks.

Starlink applications based on HOP technology can make use of the Starlink stereo networking and embed distributed micropayment and flow bandwidth service protocols into it, which not only makes the entire Starlink network completely encrypted, but also greatly reduces the data and cost settlement delay of this network.

4.2 CDN acceleration

With the rapid development of mobile Internet technology, the data flow of mobile networks presents an explosive growth trend. According to the 2020 Cisco VNI report, by 2030, the global mobile data flow will reach 89EB per month, and the mobile video flow will account for 78% of the global mobile data flow.

Every day, content providers upload thousands of video contents, which are stored in the provider's centralized database, and then are converted from the source format to the final delivery format, distributed to multiple streaming servers located in different locations of the network, and further delivered. Despite content distribution, the distance between content and users is still far away, especially in the mobile environment due to buffering problems and jitter, individual users may encounter service interruption.

HOP Protocol collects idle bandwidth resources and Internet equipment resources provided by global nodes based on blockchain technology, and obtains CDN assets through circulation on the exchange market; the demander can purchase and use the shared CDN at a price lower than the market price, which greatly saves the cost. Expanding CDN service to the mobile edge to provide distributed cache can enhance the QoE of users and reduce the use of backhaul network and core network, and all transactions and rewards are completed by HOP.

4.3 Internet of Things (IoT)

The "IoT" is still based on the "Internet", which is a network that extends and expands its clients to anything for information exchange and communication. The IoT refers to a huge network formed by combining various necessary messages about any object or process that needs to be monitored, connected, or interacted upon collection through various information sensing devices in real time with the Internet.

Blockchain nodes are deployed in each subject in the supply chain, and the data collected by sensors are written into the blockchain in a real-time or off-line manner. Such data can increase the cost of false denial of each subject. Clarification surrounding the responsibility boundary of each party should be sought and traced to its source through the blockchain structure. Additionally, keep abreast of the latest development of logistics, and take necessary response measures according to the data collected in real time so as to enhance the possibility of multi-party cooperation.

Reliance on the blockchain gateway to build the whole blockchain network is key. Based on smart contracts, asset owners can bind all kinds of locks on assets by setting rent, deposit and related rules. Through the APP, the end user pays the corresponding rent and deposit to the asset owner, and obtains the control authority (key) to open the lock, and then obtains the right to use the asset. After use, return the goods and get back the deposit.

One advantage here is accurate billing. Accurate and real-time payment can be made according to the billing standards in smart contracts, instead of rough charging. It also causes a lot of thinking, and provides an opportunity to consider potential issues in advance.

Energy transaction is based on smart meters. The main implementation method is to install smart meters at the door of each household and install blockchain software on smart meters to form a blockchain network. Users publish corresponding smart contracts on their own smart meter blockchain nodes through mobile APP, and control corresponding blockchain connections through power grid equipment provided by Siemens based on contract rules, so as to realize energy transactions and energy supply.

The HOP Protocol makes it easier to integrate and normalize data. I/O devices on today’s smart devices can easily connect traditional industrial systems and HOP Protocol networks. The gateway can connect and communicate with the terminal via Wi-Fi, WWAN and Ethernet. In addition, the processing capability of the gateway supports the intermediate equipment to summarize, convert and standardize the data from all different protocols (from ModBus, BACnet to Zigbee, etc.), and then transmit the data to the core network through the gateway. The HOP Protocol can make edge analysis on connected terminals, transfer the decision to the edge, provide real-time operations, help manage network problems, and solve network bandwidth problems by deciding whether data moves to the edge.

4.4 Internet of Vehicles (IoV) and unmanned aerial vehicles (UAV)

IoV is generally considered as a huge interactive network composed of information such as vehicle position, speed and route. The IoV services are developing and will continue to expand in the next few years. In order to have a stable development basis, we must first meet the connectivity requirements, which will rapidly increase the flow of data transmitted by sensors and processors in interconnected vehicles. Connection requirements may vary depending on the services provided, including different delay level, data proximity, computing cost and bandwidth availability.

Timely charging of electric vehicles: In this scenario, we are mainly faced with industry pain points such as complicated payment agreements, inconsistent payment methods, relatively scarce charging piles, inaccurate charging and cost measurement. We can in this scenario then launch an electric vehicle from point-to-point charging projects based on blockchain. By installing simple Linux system devices, for example, Raspberry Pi, in each charging pile, companies of several charging piles and individuals of charging piles are connected in series based on blockchain, and Smart Plug adapting to each interface are used to charge electric vehicles.

Secure communication and swarm intelligence of UAV: In this scenario, it is mainly for the rapid development of UAVs and robots in the future. The communication between machines must be considered from the following two aspects: On the one hand, each UAV has built-in hardware keys. The identity ID derived from the private key enhances identity authentication, ensures secure interaction based on digital signature communication, and prevents the spread of forged information and the access of illegal devices. On the other hand, based on the consensus mechanism of blockchain, the combination of blockchain and artificial intelligence in the future - swarm intelligence, is full of imagination.

HOP Protocol technology can be used to expand the IoV cloud to the highly distributed mobile base station environment, and enable data and applications to be deployed near vehicles. The application can run on HOP Protocol servers, which are deployed on LTE base station sites, for example, small unit sites or aggregated site locations, to provide roadside functions. HOP Protocol technology provides a platform for a new class of applications where interconnected vehicles depend. When interconnected vehicles move or communicate with roadside sensors, data and applications can still be located close to interconnected vehicles.

HOP Protocol can also provide hosting services and lower delay for applications. The HOP Protocol application can directly receive local messages from applications in vehicles and roadside sensors, analyze them, and then disseminate danger warnings (with extremely low delay) which enables nearby vehicles to receive data within a few milliseconds, thus allowing drivers to respond to them immediately.

4.5 Facing the IoT: Hybrid Fog Computing

Fog computing was named by Prof. Stolfo of Columbia University in New York. At that time, the aim was to use "fog" to stop hackers from invasion. Cisco formally proposed it for the first time, giving fog computing a new meaning. Fog computing is a distributed computing infrastructure for the IoT, which can extend computing power and data analysis applications to the "edge" of the network, and enables customers to analyze and manage data locally, so as to obtain real-time insights by connecting to the network.

In 2012, Salvador et al. put forward in an article about cloud data security that by using false information as bait, the person stealing information could be flushed out. This then proved that the protection of users' real information can be achieved. Unlike cloud computing that saves all data, data processing and applications in the cloud, fog computing disperses them in devices at the edge of the network. That is, between the cloud server and the IOT devices, network devices storage and network communication services, data and computing are closer to terminal devices, thereby reducing the computing and storage expenditure of the cloud server and improving the response speed and network bandwidth of the application system. It is called "fog computing" because fog is closer to the ground than cloud. Fog computing does not have strong computing power, because computing power is provided by the peripheral computers and scattered computing devices.

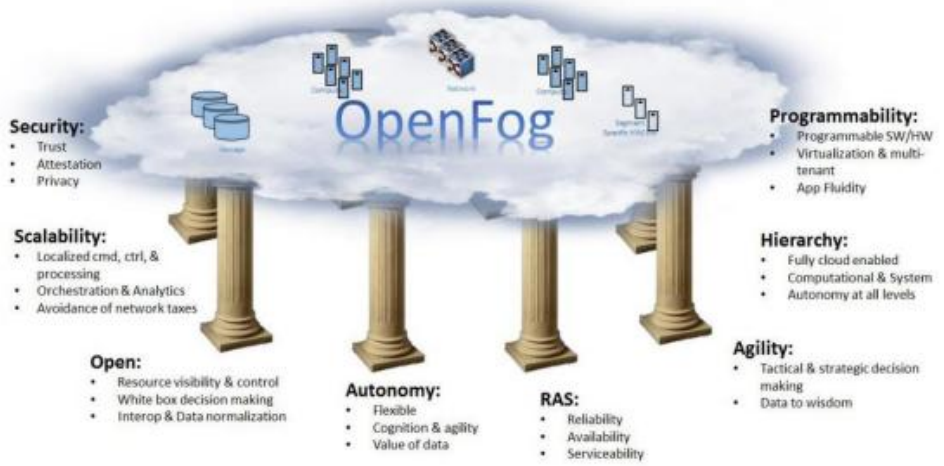


Figure 3 Open Fog Computing Value Map

In the HOP project, the characteristics of hybrid fog computing and distributed computing adopt the open part of open fog to meet the three basic requirements of HOP transmission: low delay, maintenance of user privacy and access to resources at different levels.

Fog computing is composed of network devices with weaker performance and more dispersed functions, instead of some servers with strong performance. Fog computing is a semi-virtualized service computing architecture model, which emphasizes quantity and plays a role regardless of the ability of a single computing node. Compared with cloud computing, fog computing has a more distributed architecture, closer to the network edge. Fog computing concentrates data storage, data processing and applications in devices at the edge of the network. Fog computing is a new generation of distributed computing, which complies with the "decentralized" characteristics of blockchain. Since Cisco put forward the fog computing, several major technology companies (such as ARM, Dell Inc., Intel Corporation and Microsoft Corporation) and Princeton University have joined the concept camp, and established the Open Fog Alliance, a non-profit organization, to promote and accelerate the popularization of open fog computing and promote the development of the IoT and blockchain industry.

With regard to the deployment of HOP and open fog in the HOP Protocol project, fog nodes and fog layers can be in FaaS from the perspective of infrastructure. With FaaS, each layer of locations and nodes are deployed without following a single data center. However, this does not mean that security is unnecessary. Because of distributed data storage and network topology, users and fog service providers are faced with security threats.

Security is based on "things". These things must be based on trusted hardware. This "root of trust (ROT)" must be proved by the software running on it. For being close to the end user and the edge position, the fog node must be subject to first access control and encryption, to provide integrity and isolation and control privacy sensitive data. With the emergence of more complex topology, the whole fog node "chain" must be trusted. For other fog nodes, security guarantee must be provided in the cloud. Because fog nodes are also subject to dynamic instantiation, the hardware and software resources must be reliable. Illegal components cannot participate in fog nodes. Security implementation may have many descriptions and attributes, such as privacy, anonymity, integrity, trust, evidence, hardware ROT, verification and measurement.

Fog computing architecture performs tasks related to data storage, computing, network connection and management by using a large number of edge devices and computing terminals paired with traditional cloud services. Compared with traditional architecture, fog computing architecture has the following characteristics:

(1) Conduct deployment near the location where users and businesses are concentrated for low-delay storage;

(2) The equipment, with small shape and light weight, is convenient to store and carry;

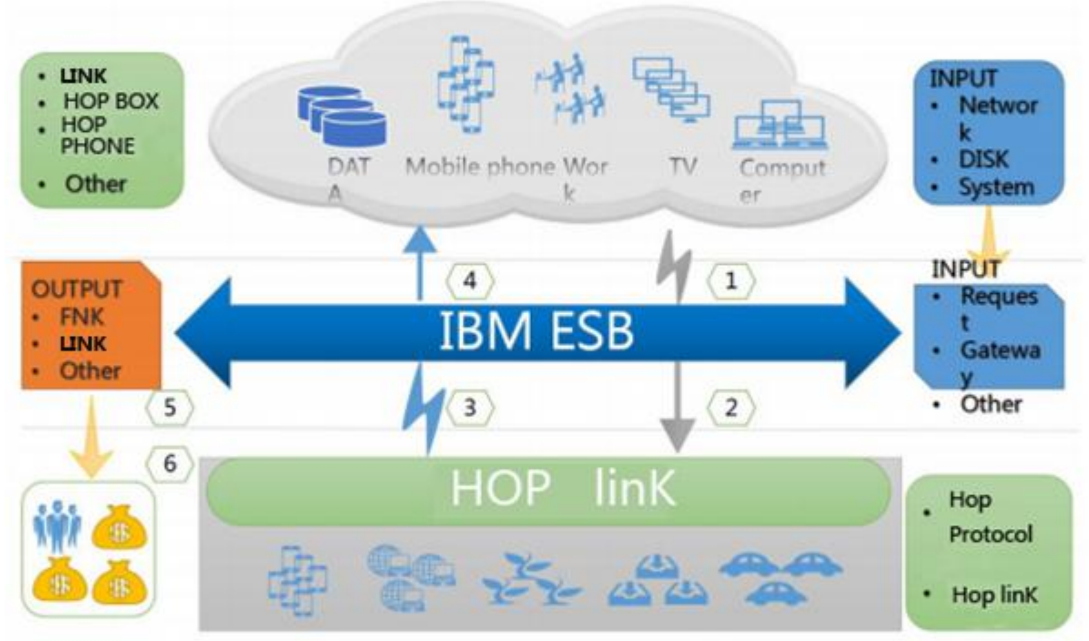
(3) The display forms of equipment are diversified, and the requirements for operating systems are low, which is convenient for transplantation;

(4) Be close to the end user, avoid delay and reduce network and bandwidth loss;

(5) Low-delay communication, instead of all communication, goes through a backbone network routing for synchronization;

(6) Implements management elements near the final node, including network measurement, control and configuration;

(7) Reliability/availability/serviceability (RAS);



Blockchain technology can be understood as follows: If we assume the database as a ledger, reading and writing the database can be regarded as a bookkeeping behavior.

The principle of blockchain technology is to find out the fastest and best bookkeeper in a period of time, to be in charge of bookkeeping, and then send this page of information in the ledger to everyone else in the whole system. This is equivalent to changing all the records in the database and sending them to every other node in the whole network, so blockchain technology is also called distributed ledger. Combined with the characteristics of fog computing and blockchain, users can submit specific disk and network resources with the fog computing device of HOP, so as to obtain HOP digital assets.

Chapter V HOP Protocol Route and Team

5.1 HOP development roadmap

Development cycle	Events/plans/milestones
Stage I Selection period of technical verification	1. The consensus protocol satisfies Byzantine fault tolerance algorithm. 2. Support mortgage HOP coins to join the public blockchain network. 3. Dilute the concept of mining pool, and any mining rig can participate in mining. 4. Quick and stable block discharging (only under the condition of 0-100 mining rigs) 5. Support transfer mining.
	The R&D cycle is 6-12 months.
Stage II Technical performance improvement period	1. The mainnet is in official running, and ERC20 tokens are mapped to the public blockchain network. 2. The public blockchain network supports smart contracts. 3. The POS consensus realizes technical modeling. 4. Support flow mining and transfer mining. 5. Support simultaneous running of 1,000 mining rigs. 6. Optimize and upgrade existing functions and systems.
	The R&D cycle is 12-18 months.
Stage III Mature development period of technology	1. Support cross-chain payment function, ETH and BTC procurement flow services. 2. Support POS+POF consensus technology. The cumulative contribution of flow can become the weight of computing power. 3. Support fragmentation technology. 4. Support free joining and quitting of the public blockchain network. 5. Improve the stability and safety of block discharging.
	The R&D cycle is more than 12 months.

Chapter VI HOP Community Autonomy

6.1 Constitutional basis of HOP community autonomy

The development team of HOP Protocol integrates the research results of the well-known public blockchain constitution and jurisprudence of the current blockchain. It also defines the constitutional basis of HOP Protocol community autonomy. As a decentralized community governance institution, it adheres to the principle of "bad behavior must be punished” and implements the decision-making of community autonomy affairs through "code as law".

6.2 HOP community governance system

The HOP Protocol is committed to decentralizing the centralized rights and interests of the project to the community, and every stakeholder and contributor can participate in the operation and development of HOP Protocol to realize the vision of true decentralization.

Objects exercising rights and interests: stakeholders holding the rights and interests of the HOP Protocol digital currency and voluntary contributors of the community

Types of rights and interests exercised: including but not limited to: application scenario proposal, application product voting, community development proposal, project development proposal and community committee election

Ways to exercise authority: on-line submission of suggestions, voting rights (consent/veto), participation rights, etc.

Rules for exercising authority: The final result is judged according to the principle of minority obeying majority within a given time range. Submission rules for exercising rights and interests include the adherence to the agreement that those receiving responses of more than 20% of the members of the current community in a specific page within a specific time may enter the voting level.

The HOP Protocol community committee members are elected by community voting. Their main functions include supervising the operation progress of various pages of the community, cleaning up invalid information, supervising the implementation of rights and interests, etc.

The functions and election methods of community committee members are as follows:

(1) Community director: Has the authority to propose a number of suggestions, organizing activities and transferring topics in the community, and is elected by the community executive and deputy directors; the term of office is one year;

(2) Community instructor: Have no community authority, only provide

community technology and service consultation, and be appointed by the founding team;

(3) Community vice chairman: Assist the director's work, carry out community autonomy, and be elected by community executives and directors; the term of office is one year;

(4) Community executives: Represent community stakeholders to issue initiatives, and supervise transparency of daily community behaviors such as various activities, topics, and voting; be elected by community stakeholders (the top six votes, from high to low); the term of office is one year.

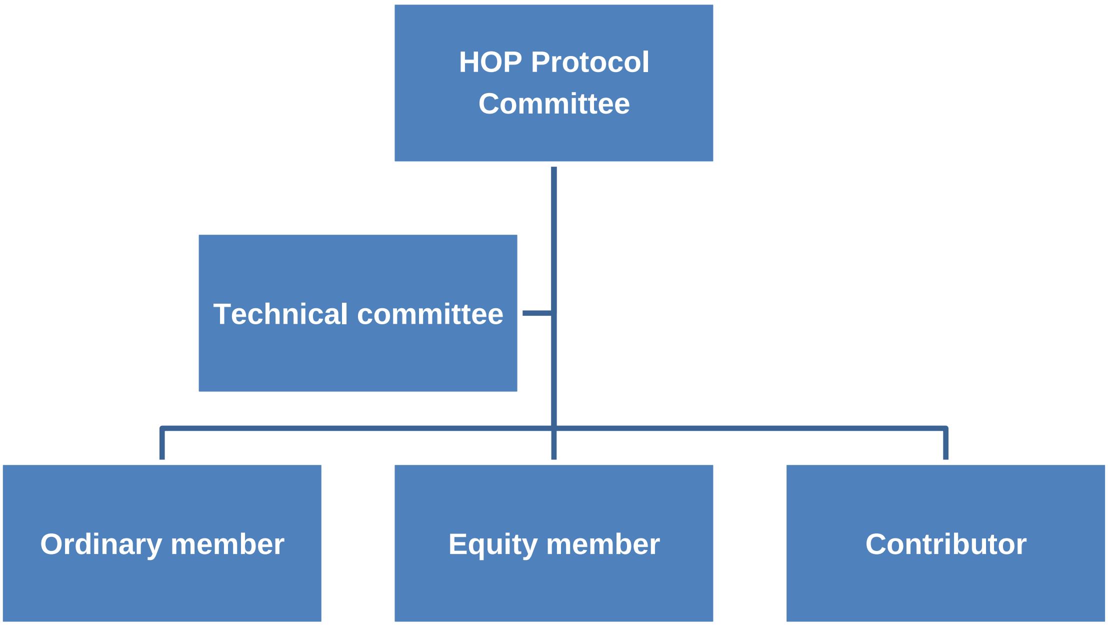
The establishment time of the first community committee of the HOP Protocol is published by the project team in the community after the digital currency of HOP Protocol is distributed. We are about to welcome more and more community members, so we have also made relevant divisions for stakeholders of the community, so as to facilitate the decision-making of the community committee in the future.

Definition explanation

Ordinary member: Register as a member of the community, to easily browse various consultations and discussions, without voting rights; gradually obtain HOP Protocol digital assets by participating in community activities, providing suggestions and business clues, and then upgrade to an equity member;

Equity member: A registered member binding the wallet address. The wallet has a certain number of HOP Protocol digital assets;

Contributor: A registered member contributing service nodes, must pass on-line authentication and identification, mainly to identify the skill proficiency, and the whole process is anonymous.



6.3 Code is law

The essence of law is "contract", and the essence of current law is a kind of contract, which is concluded by people and their leaders in the same community agreeing on ways to interact with each other. There are also some contracts between individuals, which can be understood as a kind of justice. Correspondingly, this kind of justice only takes effect for the participants of such contracts. In the world of blockchain, the intelligent contract composed of code forms the "self-rule" of blockchain and the law of blockchain, which means that code is law.

Code corresponds to words in a language, but is different from the "multiple interpretations" of words. The meaning of the code is unique. As a core tool, code can be used to build and protect the cyberspace of our most basic values, and it can also be used to make cyberspace disappear. In *Code*, Professor Lawrence Lessig repeatedly emphasized that code-based software protocols can regulate our lives like any legal rules.

In essence, a contract composed of code is an unambiguous contract that cannot be broken. As long as both parties agree with the contract, the contract will be executed, no matter whether anyone wants to break the contract or raise ambiguity. Code is the best language, and the code's self-rule will run by itself, which is a machine law that doesn't transfer people's subjective will. Therefore, the HOP Protocol thinks that code means rules.

Whether the constitution of community autonomy of the HOP Protocol can be implemented normally depends on the effective issuance of codes. In view of the principles of openness, transparency and co-construction of the HOP Protocol, the main function of the technical committee is to ensure the integrity and security of the code. Therefore, technical committees are specially set up under the community autonomy committee, and their responsibilities are as follows:

(1) Sort out and publish code rule formulation and technical management tools;

(2) Repair, test and optimize BUG and requirements;

(3) Adopt and feed back community suggestions, and reward community members;

(4) Recruit, manage and develop the developer community, and review and test the developer code;

(5) Issue code, and update all node clients;

The HOP Protocol community autonomous governance institutions need mutual supervision and balance, and all administrative affairs are implemented openly and transparently; all administrative decisions are empowered to community members.

6.4 Mining pool management committee

As an important link in the blockchain industry, the mining pool provides stable mining revenue for the majority of miners, and as a result the management and safety of mining revenue is a high priority. The HOP Protocol mining pool management committee (hereinafter referred to as "the management committee") is dedicated to the management and transparency promotion of the HOP Protocol mining pool. The management committee helps manage the general and special matters of the mining pool and open source community projects by formulating good governance institutions. At the initial stage of the project, the management committee mainly considers the sustainability, management effectiveness and safety of the project development under the large mining pool alliance. The management committee is composed of the technical team, operation team and mining pool team. The management system and community autonomy system of the management committee are two different systems. The management system of the management committee is discussed below.

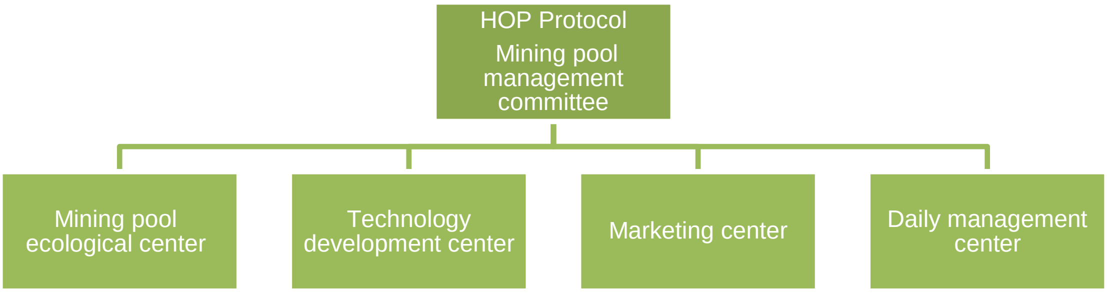
The management committee and each team have the following division of labor:

(1) The HOP Protocol management committee manages and decides major issues of the mining pool alliance, including hiring/firing executive leaders and center leaders, making important decisions, etc. The management committee shall have a president, who shall be decided by voting of the members of the committee.

(2) The operation team promotes and publicizes mining pool technologies, products, communities and open source projects, including the implementation of the community operation and promotion proposals; be responsible for personnel, finance, legal affairs, administration and other management work.

(3) The technical team is in charge of the development, test, launching, audit, and more of the underlying technologies related to the HOP Protocol mining pool. They will also regularly publish technical progress in the community, communicate the project progress with community contributors, and participate in technical exchange meetings at home and abroad.

(4) The mining pool team explores and implements the industrial application of the HOP Protocol. The main aspects of work are: mining pool implementation and operation, operational data integration, Internet financial project management and control, intelligent scheduling of platform supply and demand, etc.



HOP Protocol

Mining pool management committee

Mining pool ecological center

Technology development center

Marketing center

Daily management center

Chapter VII Risks and Disclaimers

The HOP Protocol is a non-profit organization for edge computing, development, construction and promotion.

The white paper, without review by regulatory authorities in any jurisdiction, is only used to describe the HOP Protocol ecosystem and operation mechanism, which is neither a prospectus or an offer document in any form, nor a practical investment operation proposal. The information, opinions and comments involved in the paper are not guaranteed with respect to accuracy, completeness or reliability, and are not contracts or promises in any form, which cannot be used as the basis for investment decisions.

Any institution or individual investor must strictly abide by the relevant laws and regulations of their jurisdiction, and be clearly aware of the risks of HOP Protocol. Once participating in the investment, you are deemed to have been aware of and willing to bear the corresponding risks. Participants need to complete a series of steps and provide specific information and documents, and citizens of some countries and regions will not be able to participate in this token issuance because of legal prohibition. HOP Protocol cannot guarantee that the value of tokens is bound to increase, and does not make any commitment in any form, so it has no obligation to compensate for all direct or indirect losses caused by participating in token investment. HOP Protocol is only a digital asset, which does not represent the ownership or control of the project. Even if you have a considerable number, you do not have any decision-making about the project.

According to the external environment and the R&D progress of the project, the contents of the white paper may be modified or supplemented at any time, without further notice. Please track the update situations in time through the official website of HOP Protocol and relevant communities.

In view of the high risk coefficient of digital asset investment, please carefully review the investment agreement and comprehensively assess the risks and affordability.