



# SoFa-Network Wormhole network

## Project White Paper v0.2

(Non-final version, some of the content may be modified)

SoFa-Network Technical team

SoFa-Network foundation

Establish

# Category

<b><i>I. Introduction .....</i></b>	<b><i>4</i></b>
<b><i>II. Project background .....</i></b>	<b><i>8</i></b>
2.1 Unconnected Internet .....	8
2.2 The Insecure Internet.....	14
2.3 The Uneconomic Internet.....	17
<b><i>III. Project Introduction .....</i></b>	<b><i>21</i></b>
3.1 Project Positioning .....	21
3.2 Project Prospects .....	22
3.3 Project Progress .....	24
<b><i>IV、 Technology achievements .....</i></b>	<b><i>26</i></b>
4.1 Multi-p2p-Protocol Network.....	29
4.2 Dynamic No-Key-Exchange Transport Layer Security .....	37
4.3 SoFa Decentralized Name System.....	38
4.4 Proof of Packet .....	39
4.5 Expected Consensus .....	42
<b><i>V. The economic model.....</i></b>	<b><i>45</i></b>
5.1 Token Introduction .....	45
5.2 IMO Plan.....	46

5.3 The Auction Mechanism .....	47
5.4 Public beta plan.....	47
5.5 Foundation Operation .....	48
<i>VI. Project Team</i> .....	<i>50</i>
6.2 Foundation .....	51
6.3 Community .....	51
<i>VII. Risk Prompt</i> .....	<i>54</i>
7.1 Legislation risks .....	54
7.2 Market risks.....	54
7.3 Attack Risk.....	55
7.4 Technology Risks .....	55
7.5 Risk of using.....	56

# I. Introduction

In March, 1989, the father of Internet, Tim Berners-Lee, officially put forward the conception of World Wide Web(WWW) and the first web browser of the world was developed in the European particle physics laboratory in Geneva in the next year. After 30 years of rapid development, the number of Internet users in the world has exceeded 4 billion, accounting for more than half of the total population of the world. From the analog signal network to the Fiber-optic communication network and then to the mobile communication network, the transmission medium and the transmission speed of the data on the Internet realize the leap of the large span. Internet-based business models and network services have also reached an unprecedented level of prosperity. It took human beings a short period of 30 years to enter the information age from the industrial era as a whole and is striding forward to the digital age.

However, in the process of advancing to the digital age in the information age, we face many difficult problems. Among these problems, some are controlled for human purposes, some are limited by natural conditions, some are limited to the bottleneck of technological breakthrough, and the others are the network structure and business paradigm that depend on and rely on in the process of starting to mature in the information age have been difficult to meet the needs of the development of the digital age. We look at the interconnection of everything, strong artificial

intelligence, explore the universe and other great vision to outline the blueprint of a better life for mankind in the future, but trapped by the existing unconnected Internet, not secure enough, not enough economic dilemma. So no matter how eager we try artificial intelligence or the Internet of things and other new technologies, they will eventually become a dream bubble, empty sigh and disappointment.

In order to solve the real problems existing in today's Internet world, we are also glad to see that countless pioneers have made unremitting explorations with their wisdom and efforts. In 2008, the ravages of the global financial crisis revealed to the world the ugly way for powerful countries to harvest wealth and pass on risks through seigniorage. A password geek, alias Nakamoto-Cong, showed us the charm of decentralized currency issuance and accounting with the *One-to-point electronic cash system* and the subsequent release BTC network that operate stably for ten years. Ethereum brings smart contracts into the blockchain network with its genius. The idea of code and law, like a crack in glass, begins to break down a power-based contractual society into a code-based consensus society. Ethereum also shows the charm and advanced nature of blockchain to the

world because of its strong landing at the financial level. In 2014, a group of young graduates from Stanford University creatively put forward the concept and vision of IPFS in order to solve the problems at the bottom of location-based content storage in the Internet world. And worked hard for it for more than five years and attracted the participation of hundreds of developers and hundreds of thousands of investors around the world. In January 2015, SpaceX of Silicon Valley Iron Man Elon Musk proposed a Starlin plan, the approval of the Federal Communications Commission was formally approved in 2019, opening a formal space networking prelude to providing high-quality communications services to any corner of the Earth through communications satellites throughout Earth orbit.

All these great achievements like a burning torch to illuminate the path of the Internet world. We also hope to be able to work with many pioneers to lay a solid step on the road to a better world in the future. Therefore, I worked with several like-minded colleagues and friends to launch the design and research and development of SoFa-Network in 2017. After nearly 2 years of research and development, the overall architecture design of SoFa-Network has been taken shape. The mathematical proof of core

technology and the realization of code have been basically completed. The development and perfection of supporting technology and supporting tools have also been started. Now, we will show the world our first stage of R & D results and landing products. In this process, we are particularly grateful to early investors and enthusiasts for their attention, trust, support and patience, so that we can focus on solving technical problems and breakthroughs. It's also an honor to get investment and help from communities and institutions in the blockchain to turn advanced technology into landing products. A lot thanks to the community for taking over the operation of the project, so that we can focus on the technical areas we are best at and love most. Special thanks to colleagues who have given up high-paying jobs and family time over the past two years. It is your long-term efforts to make SoFa-Network finally gets an opportunity to say:

**Hello, World !**

## II. Project background

SoFa-Network was created to address the three major problems of insufficient connectivity, security and economy that now exist on the Internet. The reasons for the formation of these three major problems are different and complex. However, it greatly limits the evolution of the Internet world one step further. Only by understanding the causes and nature of these three problems can we better optimize the underlying network structure and support a richer and diverse Internet ecology.

### 2.1 Unconnected Internet

The existing Internet is an inextricably and closely linked world. However, in fact, there are many local areas that cannot be accessed, restricted access, access rights are controlled by people and so on. To a certain degree, the Internet has been separated and isolated, closed and controlled, which has long been contrary to the ideal and original intention of the Internet.

Although the number of Internet users in the world has exceeded 4 billion, the number of people who do not have access to the Internet is still more than 3 billion. Among these 4 billion



Internet users, there are a very high proportion of users cannot fully access the Internet all or there is a risk of inaccessible. There are many limitations and uncertainties in access type, access object and access mode.

Let's take the African region as an example to get to know the Internet, which is not connected enough. According to public data, only about 388 million of the continent's 1.25 billion people have access to the Internet, with less than 30% of Internet access. Nearly 800 million Africans are still unable to enjoy the good life brought about by the Internet. For many areas and users of the continent, this is not a truly connected Internet.



There are three main manifestations and causes of this problem:

Firstly, The African continent is vast the geographical environment is very different, and the geographical environment is very bad in many regions. The level of political, economic and cultural development among regions are different, resulting in great imbalance in the construction of Internet infrastructure such as optical fiber and base stations on the African continent. Under such natural and economic constraints, many parts of the continent are in the vacuum of the Internet world.

Secondly, Due to the poor geographical environment and backward economic level, it is difficult for the Internet infrastructure construction on the African continent to break through the critical point of scale effect and the marginal cost curve of network services is very smooth. The direct consequence is that most people are too expensive to use the Internet even in areas with Internet infrastructure. Take broadband access alone as an example, South Africa has the highest broadband access rate of \$7.6 / GB, Kenya \$4.9 / GB, Nigeria \$3.1 / GB. Such a high cost of surfing the Internet has greatly limited the use of the Internet in Africa.

Thirdly, the network censorship system is widespread in various countries in Africa and the degree of network review varies from country to region. As shown in the following figure:



The various countries in the world have more or less reviews of network access due to political, economic, cultural and network security. The most censored regions, such as Somalia, on the African continent, North Korea on the Asian continent, have almost prevented regional users from properly accessing the open Internet world. The existence of this kind of censorship system, on

the one hand, protects the security and cleanliness of the network area in the complex global Internet world. On the other hand, it also limits some of the rights of users in the region to freely access the Internet. Form large or small isolated islands in the whole connected Internet world.

In addition, the existing Internet world is set up on 13 root services that based on DNS (domain name system) to operate effectively. However, of the 13 root servers, one primary root server and nine root servers are in the United States. There are only three root servers outside the United States, one in Japan and two root servers in Europe. The United States has the monopoly hegemony of the global Internet, which does not rule out the possibility of interrupting Internet access in some countries out of its own interests. It is also a sword of Damocles hanging over the head of today's Internet world, and the United States is the swordsman.

The above-mentioned problems of the Internet are not interconnected, and in most parts of the world. The cause of these problems lies in the topological structure and business paradigm of the whole network in the information age. Almost all the existing Internet services are C/S or B/S centralized architecture,

including the global DNS domain name system, which is also the centralized service. The network topology has led to strong governments and enterprise to undertake the cost of large infrastructure construction in the early development of the Internet. For example, the construction and maintenance of DNS server, the laying and maintenance of fibre link, the construction, maintenance and upgrading of base station all need a lot of funds and technical strength to carry out. In such supply and demand relationship, the government and enterprises will measure the efficiency of input and output. A lot of money will not be invested in infrastructure construction in countries and regions have poor natural environment, scare population and low level of economic development. On the other hand, it is precisely because the infrastructure of the Internet is almost done by strong governments and enterprises, which makes them form strong control over the network path, and then breed the ultimate control mode, such as high rate, network censorship and network attack. In the end, the fragmentation and distortion of the connected world will be difficult to deal with.

0000 0000 00000000 00000000

In June 2013, Edward Snowden, a former CIA technical analyst, disclosed secret NSA documents about the PRISM surveillance program to the *Guardian* and the *Washington Post*, followed by the UK's secret intelligence surveillance program, causing a worldwide stir. It is an open secret for government intelligence agencies to spy and steal information on their citizens and other government departments through the Internet. WikiLeaks' revelations of state leaders, government executives being monitored, the theft of multinationals' trade, and technical secrets through surveillance are also shocking.

All kinds of events, let the hearts of people in the Internet world shrouded in a lingering shadow. Even if people are willing to pay additional costs for more secure network communication services, they still cannot eliminate the hidden dangers of information listening and stealing from the underlying technical level. Mobile phones, routers, base stations and other hardware leave back doors, systems, software, firewalls can secretly monitor people's life. Email is not secure, social software is not secure, and behavior records on the Internet are also analyzed by various big data methods. We are in an era of comprehensive progress from

an atomic society to a digital society. In the future, all human beings, including identity, property, social relations, personality will exist in the form of numbers and flow on the Internet. However, people have not yet found an effective way to dispel people's concerns about information security from the technical and mathematical levels. It makes it possible for people to make a shudder at the entrance to the digital world from the atomic world:



It is said that the information that is currently present in the Internet world, monitoring and theft, only makes us feel that privacy is offensive and business secrets are threatened. Then, in the era of rapid progress in the Internet of things, insecure

Internet will pose a great threat to the lives and property of all people. Driving cars, smart home equipment, unattended warehouses and automated factories, communication between machines will be everywhere. Once the information in a certain part of the network line is stolen or tampered with, it will lead to very serious consequences. With the continuous entry of human beings from the atomic world into the digital world, cybercrime and cyber warfare will also become the main harm to the overall survival and security of mankind in the future. How to protect their own information security is a subject that every human individual must face. How to protect the network security of an organization, region and country is also the defense focus of enterprises, governments and countries in the future.

However, according to the current situation of the underlying network, it is difficult for individuals and organizations to completely protect themselves from cyber violence and attacks. The centralization of app services has enabled monopolistic giants such as Google and Facebook to wantonly steal users' private data for commercial purposes. The centralization of basic network services gives the world's top communication operators, such as AT&T, Verizon, China Mobile, a huge right and the standard and



pricing of space to control the communication network, as well as the admission control and violation authority of all kinds of hardware devices derived from it. In such a highly centralized network of hardware, systems, networks, software, and applications, users must pay a high price to protect their information security. For example, onion protocol, VPN, asymmetric encryption technology and so on. However, technology such as asymmetric encryption is difficult to apply to people's daily network communication because of its consumption of computing resources. Therefore, these technologies can only protect the information security of users in specific scenarios and needs.

## **2.3 The Uneconomic Internet**

After entering the 21 st century, many countries and organizations began to mention the concept of Internet economy more and more frequently. In the early days, Internet economy refers to saving human, material, financial, time and space resources through the tools and methods of the Internet, and obtaining greater results and benefits. Under the guidance of this simple Internet economic ideas, the Internet has been tried to

reduce the production, service and transaction costs of various industries. Such as internet newspapers and magazines (early portals), internet bazaars (early e-commerce), internet meetings (early communication software and co-office software).

With the continuous upgrading of Internet technology, the continuous reduction of use costs and the increasing variety of application services that the Internet can carry, the number of Internet devices and users in the first 20 years of the new century has produced a sustained explosive growth. According to Metcalfe's law, the value of the network is equal to the square of the number of nodes in the network, and is proportional to the square of the number of users on the network. The value of the Internet in this exponential growth process has proved to the world that the Internet value is more than one way to interpret and the value of the Internet itself has even begun to go beyond the value of other industries. As a result, the Internet economy has entered the era of real network economy, and the Internet economy has also become a new, valuable and promising economic ecology. It has changed almost all the lifestyles and ideas of people, such as food, clothing, housing and transportation, and

has also spawned countless new business models and more than a dozen Internet giants from rich and enemy countries.

However, because of the underlying structure of the Internet and the business paradigm of the free economy, the current Internet economy has become less economical.

First, the centralized network architecture determines that the limited network basic service providers (such as communication operators, data centers, cloud storage cloud computing service providers, etc.) carry the access needs of more than 4 billion users around the world, which created the so-called information superhighway, but a very crowded low-speed road. To respond effectively to the increasing variety of network services, these limited network basic service providers need to spend a lot of cost to increase the number of concurrency and data that the server can carry. At the same time, there are a lot of bandwidth resources wasted in the client network. The Internet has gone from economies of scale to the stage of uneconomic scale.

Second, the existing Internet architecture is destined to be ultimately by some giants to control a certain aspect of the service. Almost all the business paradigm of the Internet is to become a giant or join the giant camp as the essential model. To

gather a large number of users, data, talents, funds to build a moat to become a giant, the state, enterprises, capital institutions all spare no effort to carry out regional protection, subsidy wars, money-burning marketing and other acts that violate the normal business logic.

Today, the Internet economy presents a zero-sum game and even lose-lose situation that no one wants to see. The high cost of the network and the cold moat have also stifled a large number of grassroots enterprises that want to innovate and start businesses based on the Internet.

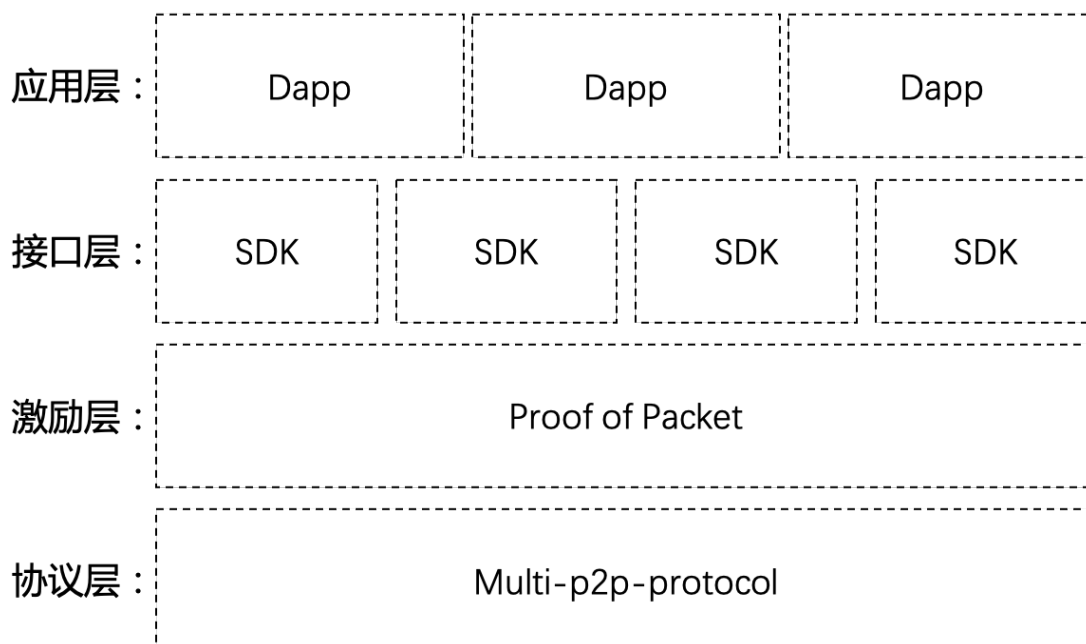
Based on this problem, we launched the SoFa-Network project. We try to build a decentralized distributed Internet infrastructure by combining blockchain technology with new network underlying protocols. And support all kinds of enterprises and developers to develop a variety of applications based on SoFa-Network to achieve a distributed Internet business world.

## III. Project Introduction

### 3.1 Project Positioning

SoFa-Network (wormhole network) is an Internet underlying communication infrastructure which combines network communication protocol, block chain book and application layer SDK. SoFa-Network builds a dynamic multi-protocol MPN network (Multi-p2p-Network) through the self-developed Multi-p2p-Protocol. It is proved by Proof of Packet packet transmission that the packet transmission exchange between network nodes is signed and accounted for. The value transfer between nodes in the network is quantitatively counted and settled by block chain. Based on MPN, a wealth of SDK, is provided to support the development and landing use of all kinds of applications based on SoFa-Network.

## SoFa-Network 项目架构说明



The SoFa-Network Foundation will also build a stronger decentralized communications network from the network physical layer and link layer by laying out new network infrastructure, such as participating in StarLink, 5G infrastructure projects. By then, SoFa-Network hopes to become the world's fourth largest communications operator after AT&T, Verizon, China Mobile and the first decentralized blockchain operator in the world.

### 3.2 Project Prospects

As a new network infrastructure, SoFa-Network can support rich blockchain applications. As a decentralized, untampered, point-to-point network infrastructure, SoFa-Network is more

acceptable to the web3 world than traditional network communication operators. SoFa-Network will launch a three-stage version according to the progress of the development.

#### Phase I: wormhole

SoFa-Network wormhole can realize the function of decentralized network agent and network acceleration on the preliminary MPN network. Wormholes can establish fast and private data transmission channels and micro-payment channels between any two MPN nodes in the world. Wormhole can make full use of many idle communication resources in edge and terminal networks around the world to provide users with traffic agents, traffic acceleration and CDN services. In theory, users can access any public network service in the world through wormholes and the access has the characteristics of high speed, high stability, and private security.

#### Phase II: Zhizi

SoFa-Network Zhizi can support third-party developers and enterprises, develop point-to-point encrypted chat tools based on MPN, encrypted video real-time calls and other applications. Different from the traditional encrypted chat tools and video call applications, SoFa-Network can realize point-to-point connection

without server and relay and the connection can realize dynamic switching, automatic line optimization, multimedia protocol support and so on. The difficulty of cracking encrypted content is the same as that of cracking Bitcoin.

### Phase III: phantom

SoFa-Network phantom can be used as a decentralized blockchain communication operation network. Any individual or organization can use SoFa-Network phantom to access their own devices to provide communication services for other users on the network. Phantom is committed to becoming a new generation of inter-network clearing systems and network clearing systems, which is capable of accessing between optical, mobile and satellite communications. Besides, it can make all kinds of traditional communication operators to provide communication services to users outside the network and real-time settlement.

## **3.3 Project Progress**

The first stage wormhole version of SoFa-Network has been developed and is in the internal testing stage. It will be open for public testing and commercial landing on September 1, 2019. The



two other versions will be online in turn within a year. At the same time, SoFa-Network also received some ecological contributions from third-party developers to develop Dapp based on wormhole versions.

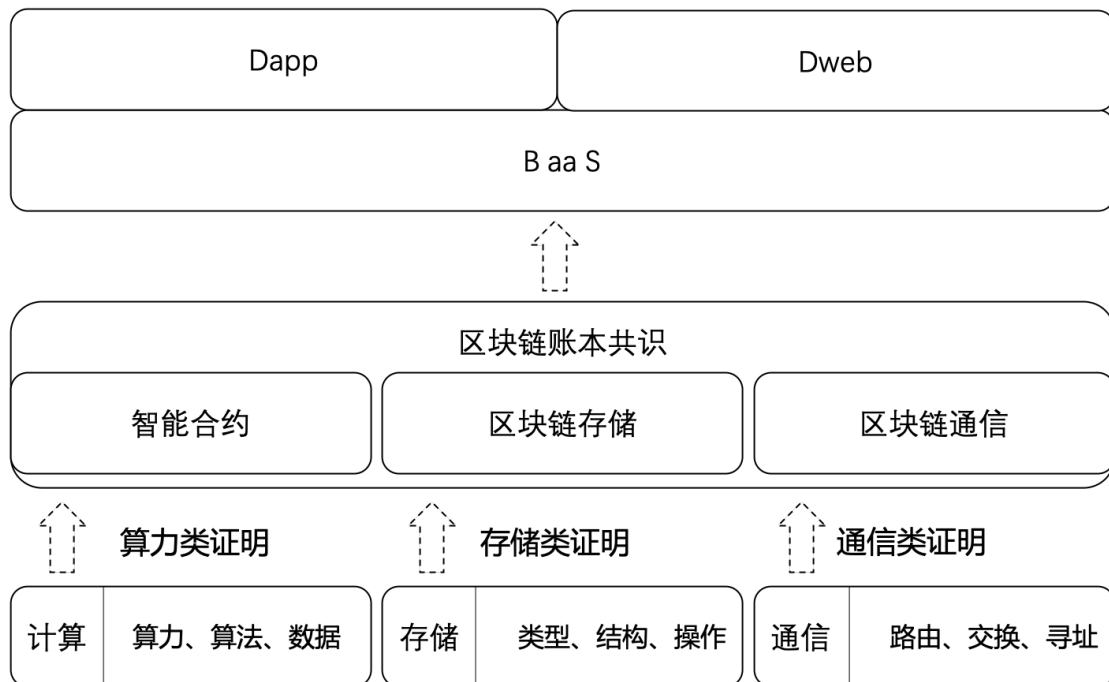
## IV、 Technology achievements

SoFa-Network is a complete decentralized network infrastructure solution rather than a simple blockchain project. Most of the existing blockchain projects are based on the introduction of block chain books into existing network applications to achieve token de-centralization accounting and incentive. Yet, this type of block chain project, in addition to being able to land at a certain level at the financial level, has little to do with real Internet business.

Taking Bitcoin for example, the data structure and consensus mechanism of Bitcoin are destined to be used only as currency. Networks such as latcoin and BCH,BSV, which are derived to improve the performance of Bitcoin, still do not change the inherent genes of Bitcoin. Alough many developers around the world try to develop all kinds of new network applications based on Bitcoin network, these applications are essentially payment and settlement applications characterized by Bitcoin replacing sovereign currency.

Ethernet network can achieve richer applications than Bitcoin network because of the innovative introduction of intelligent

contract mechanism. The innovation of real Internet applications requires upgrading and centralization of the underlying architecture, not just the de-centralization of recording books. The core elements of the Internet are mainly computing, storage and communication. The degree it can support the landing operation of the corresponding block application depends on to what extent a common chain can transform the three elements of the bottom to make it chained. Bitcoin is essentially centralizing the consensus on accounting books only through the POW mechanism. On this basis, ETH took a small step forward. The essence of intelligent contract is to link computing power and algorithm block to a certain extent, so that the code contract of code and law can be realized. However, no matter Bitcoin or Ethernet Square, what has been done in the computational blockchain transformation is still very primary and it is not involved for the underlying storage and communication. That's why Bitcoin and Ethernet are able to shine in money and finance, respectively, but show incompetence when it comes to slightly more complex applications.



We are also pleased to see more public chains trying to transform computing, storage and communication into more chunks. Sia Coin attempts to combine PoW with storage for blockchain storage. IPFS and Filecoin go a little further at this point, hoping to invent a new storage-based certification mechanism, PoRep, PoSt, to completely centralize the storage layer. Orchid protocols, TON and other projects are also trying to transform communications into blockchain, but there is no effective solution to land.

The Sofa-Network has summarized the advantages and problems of the above-mentioned various block-chain design ideas and architectures. At the same time, it also summarizes the

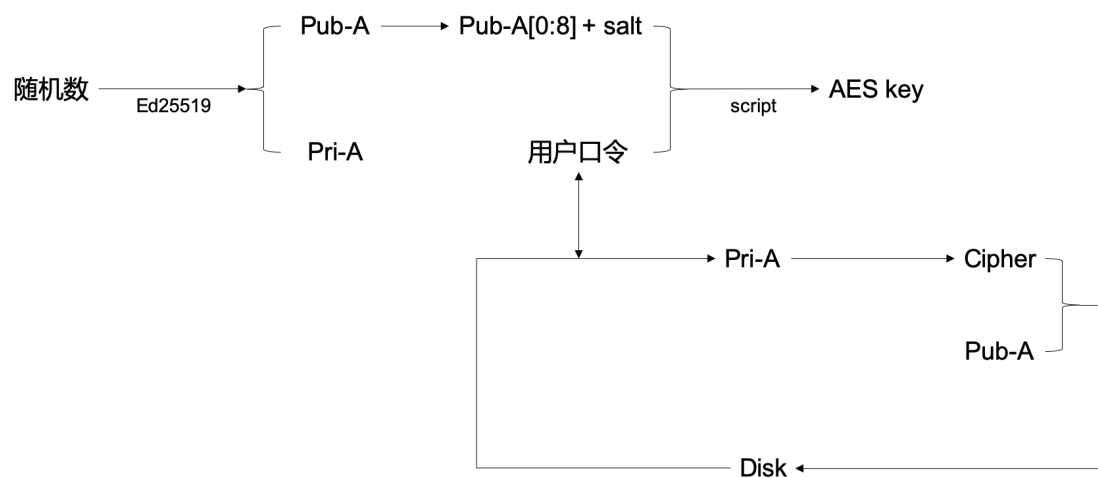
characteristics and disadvantages of the existing related technologies and protocols and is committed to the complete blockchain of the underlying communication. Thus, we have read a large number of research papers and carried out long-term and tedious mathematical proof. After repeated research, proof and code test, we creatively designed the core technical architecture and components of SoFa-Network from the shoulders of our predecessors.

## **4.1 Multi-p2p-Protocol Network**

The Multi-P2p-Protocol Network (MPN) is a p2p network that supports multi-protocol types through encryption and p2p protocols. We deeply study the protocol principle and implementation of many kinds of protocols used to construct P2P network and find that there are many problems in the process of practical application of the existing P2P protocol. For example, the node credit system is not perfect, the NAT penetration rate is low, the relay node dependency is high, the node discovery and the node addressing efficiency are low, and the like. On the basis of rigorous papers and mathematical proof, we almost completely independently reconstruct and perfect most P2P protocols to solve

their problems, so that we can adapt to a variety of complex network environment.

MPN randomly generates a pair of public and private keys as the unique identity of nodes in MPN networks by random number algorithm and asymmetric encryption algorithm Ed25519. Each node has a unique public key address to represent its identity in the network and a private key to prove the corresponding identity. Through the conversion of key pairs, the protection of password security is strengthened and the complexity of user operation is reduced.



After the node is generated, it will bring its own node information (including public key, node IP, network type, communication protocol, bill, etc.) to the network and broadcast its own node information. The nodes in the network maintain the

normal operation of the network through the improved DHT protocol, Kad protocol and Gossip protocol.

---

### 1 Subscription management

---

Upon subscription of a new subscriber  $s$  on a contact node  $contact$

*{The subscription of  $s$  is forwarded to all the nodes of view}*

**for** all nodes  $n \in \text{PartialView}_{contact}$  **do**

Send( $n, s, \text{forwardedSubscription}$ );

**end for**

*{ $c$  additional copies of the subscription  $s$  are forwarded to random nodes of view}*

**for** ( $j=0$ ;  $j < c$ ;  $j++$ ) **do**

Choose randomly  $n \in \text{PartialView}_{contact}$

Send( $n, s, \text{forwardedSubscription}$ );

**end for**

---

[1]Node online,[2]node subscription message delivery.

---

### 2 Handling a forwarded subscription

---

*{ $n$  receiving  $s$  adds it with the probability  $p = 1/(1+\text{size of PartialView}_n)$ }*

with probability  $p = 1/(1+\text{size of PartialView}_n)$

**if**  $s \notin \text{PartialView}_n$  **then**

PartialView $_n$  = PartialView $_n$  +  $\{s\}$ ;

**else**

Choose randomly  $n \in \text{PartialView}_n$

send( $n, s, \text{forwardedSubscription}$ );

**end if**

---

$$w_{out}(i) \leftarrow \sum_{j \in succ(i)} w_{ij}, \quad \forall j \in succ(i) : w_{ij} \leftarrow \frac{w_{ij}}{w_{out}(i)},$$

$$w_{in}(i) \leftarrow \sum_{j \in pred(i)} w_{ji}, \quad \forall j \in pred(i) : w_{ji} \leftarrow \frac{w_{ji}}{w_{in}(i)}.$$

[3]The probability relationship between dynamic Real-time Update Node and

Node

$$D(P||Q) := \sum_{i,j} p_{ij} \log \left( \frac{p_{ij}}{q_{ij}} \right).$$

[4] *The dynamic update algorithm has been proved to be convergent.*

---

### 3 Updating arc weights

---

$W_{ij}$  on node  $n_i$  contains the weight associated with the arc( $i, j$ )

$W_{ji}$  on node  $n_i$  contains the weight associated with the arc( $j, i$ )

$W_{in} = \sum_{j \in \text{InView}_{n_i}} W_{ij}$  ;

$W_{out} = \sum_{j \in \text{PartialView}_{n_i}} W_{ji}$  ;

{Update weight associated with incoming arcs}

**for** all  $n_j \in \text{InView}$  **do**

$W_{ji} = \frac{W_{ji}}{W_{in}}$

Send( $n_j, W_{ji}$ , WeightUpdate);

**end for**

{Update weight associated with outgoing arcs}

**for** all  $n_j \in \text{PartialView}$  **do**

$W_{ij} = \frac{W_{ij}}{W_{out}}$

Send( $n_j, W_{ij}$ , WeightUpdate);

**end for**

---

### [5] *Dynamic update node weight*

---

#### 4 Indirection mechanism for finding a contact node

---

Upon subscription( $s$ , Counter <sub>$s$</sub> , newSubscription) of a new subscriber  $s$  on a node  $n_i$

**if**  $n_i$  is the initial contact **then**

Counter <sub>$s$</sub>  = 2 \* Card(PartialView <sub>$n_i$</sub> )

{Initialise the length of the walk to reach a random node}

**else**

**if** Counter <sub>$s$</sub>   $\neq$  0 **then**

{Normalize weight  $W_{ij}$  of  $n_j \in \text{PartialView}$ }

**for** all  $n_j \in \text{PartialView}$  **do**

$W_{ij} = \frac{W_{ij}}{W_{out}(n_i)}$

**end for**

Choose  $n_j \in \text{PartialView}$  with probability  $W_{ij}$

Decrement Counter <sub>$s$</sub> ;

Send( $n_j, s$ , Counter <sub>$s$</sub> , newSubscription);

**else**

$n_i$  acts as the contact node and applies the basic SCAMP algorithm described in algorithm

1

**end if**

**end if**

---

[6] *Forwarding node information to avoid over-bloated single node*



MPN solves the following common problems in P2P network through the optimization of protocol algorithm.




































- NAT penetration problem: MPN reconstructs the ICE framework according to various network environments. So that all kinds of nodes in NAT environment can carry out point-to-point direct communication;
- Relay node dependency problem: The MPN improves the Gossip protocol so that the MPN does not need to depend on the relay node. It can carry out large-scale networking and maintain the stability of the network, which prevents the network damage and node loss caused by the loss of relay nodes.
- The routing efficiency problems: Because the routing of P2P network is maintained by all nodes and there is no centralized routing maintenance, most P2P networks have a great burden on node resources and communication load. MPN improves DHT and Kad protocols, which makes the maintenance of network routing layer simpler, the resource occupation is lower, and the routing efficiency is also improved.



















```
[root@vultr ~]#
[root@vultr ~]# sofa debug gossip

-----YP3epyrrAfWo575kKjCMFjX6mmftgpu4uMBckF9vXXRrhC-----

*****OUT(7)*****
|||||
|YP3NUtzPcdrXA5UWo5uiFdoKM8m8neENEjWYtYiyJaqeA6|
|remoteIP      :      155.138.149.190|
|probability   :      0.17|
|HeartBeat     :      2019-06-28 09:45:45|
|direction     :      1|
|||||
|YP24ksGzGWhj3oCqKNfeWs4ENR6uYWZPVgx1Sdn2T7p4iJ|
|remoteIP      :      155.138.200.42|
|probability   :      0.17|
|HeartBeat     :      2019-06-28 09:45:45|
|direction     :      1|
|||||
|YPGaAPVtmBd97Xz8Lnb4y2FRWbkXs7Ror5AhvSrnXMUfCJ|
|remoteIP      :      155.138.211.41|
|probability   :      0.17|
|HeartBeat     :      2019-06-28 09:45:45|
|direction     :      1|
|||||
|YPFwrDThmsnLPAVBzTxDWcUrJcP58RcFD43eWwVaDj14fW|
|remoteIP      :      140.82.60.194|
|probability   :      0.17|
|HeartBeat     :      2019-06-28 09:45:45|
|direction     :      1|
|||||
|YPAXFu14PWeYrMFaYnUcfMEuiWV2wx9CnMA6fAy4PnkWa2|
|remoteIP      :      139.180.172.124|
|probability   :      0.17|
```

The following are some of the papers and proof process,  
detailed papers, proof process, algorithm implementation please  
refer to GitHub.

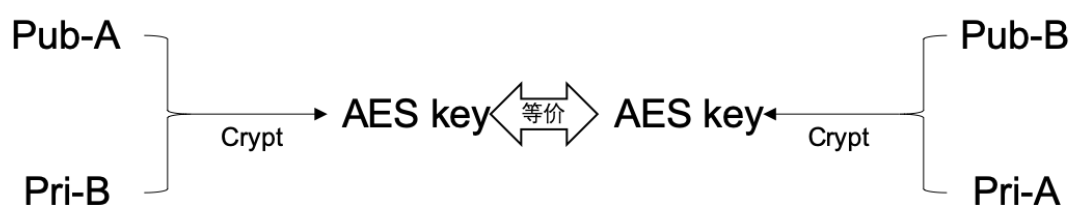
ファイル名	サイズ	形式	アップロード日時
 9781933019543-summary.pdf			
 <b>A COMPARATIVE STUDY OF GOSSIP MEMBERSHIP PROTOCOL.pdf</b>			
 composing standard gossip protocols for live video streaming.pdf			
 Correctness of a Gossip Based Membership Protocol.pdf			
 fast gossip by short message.pdf			
 Gossip and Epidemic Protocols.pdf			
 Gossip-Based Ad Hoc Routing.pdf			
 Gossip-based Protocols for Large-scale Distributed Systems.pdf			
 gossip.pdf			
 HyParView- a membership protocol for reliable gossip-based broadcast.pdf			
 IMPLEMENTATION AND PERFORMANCE TESTI...OSSIP-BASED COMMUNICATION SYSTEM.pdf			
 Information Theoretic Methods in Probability and Statistics.pdf			
 Intrusion-Tolerant Dissemination in Large-Scale Systems.pdf			
 keeping track of the latest gossip in message-passing systems.pdf			
 Peer-to-peer lightweight membership service for large-scale group communication.pdf			
 Peer-to-peer membership management for gossip-based protocols.pdf			
 Peer-to-Peer Systems and Gossip Protocols.pdf			
 PERFORMANCE OF AN INTRUSION-TOLERANT GOSSIP PROTOCOL.pdf			
 Probabilistic Reliable Dissemination in Large-Scale Systems.pdf			
 SCALable Multicast Protocol for Communication in Large Groups.pdf			
 Secure routing for structured peer-to-peer overlay networks.pdf			
 self-organizing hierarchical membership protocol.pdf			
 T-Man- Gossip-based Overlay Topology Management.pdf			
 The Effect of Network Topology on the Spread of Epidemics.pdf			
 The Promise, and Limitations, of Gossip Protocol.pdf			
 Approximate Matching for Peer-to-Peer Overlays with Cubit.pdf			
 Autonomous NAT Traversal.pdf			
 Content Availability and Bundling in Swarming Systems.pdf			
 Deployment of NAT vs. IPv6 in BitTorrent.pdf			
 Implementing NAT Traversal on BitTorrent.pdf			
 Measuring Large-Scale Distributed Systems- Case of BitTorrent Mainline DHT.pdf			
 NATBLASTER- Establishing TCP Connections Between Hosts Behind NATs.pdf			
 Peer-to-Peer Communication Across Network Address Translators.pdf			
 Session Traversal Utilities for NAT (STUN).pdf			
 TCP Connections for P2P Apps.pdf			

-  3-4.3.pdf
  -  3-kademia.pdf
  -  2823ca71520038773346b6e5bbfadc5c8419.pdf
  -  BitTorrent\_DHT\_security\_assessment\_ntms11.pdf
  -  coral-iptps03.pdf
  -  coral-nsdi04.pdf
  -  Diss.Kohnen.pdf
  -  download.pdf
  -  Kademia\_Guide.pdf
  -  Kademia- A P2P Informa2...sed on the XOR Metric .pdf
  -  maymounkov-kademia-Incs.pdf
  -  security.pdf
  -  SKademia2007.pdf
- 
-  curves-2017-c6.pdf
  -  Elliptic Curves Number Theory And Cryptography 2n.pdf
  -  EthsnarkPrecompile.pdf
  -  Explaining SNARKs Part VII\_ Pairings of Elliptic Curves – Zcash Blog.pdf
  -  Exploring Elliptic Curve Pairings – Vitalik Buterin – Medium.pdf
  -  Improved zk-SNARK Multi-party Computation Protocol – Zcash Blog.pdf
  -  l\_4.pdf
  -  MScThesis\_DennisMeffert.pdf
  -  Quadratic Arithmetic Programs\_ from Zero to Hero – Vitalik Buterin – Medium.pdf
  -  RezaAkhtar.pdf
  -  ShortNIZK.pdf
  -  slides\_smith.pdf
  -  slides\_smith2.pdf
  -  talk-96.pdf
  -  Zk-SNARKs\_ Under the Hood – Vitalik Buterin – Medium.pdf
  -  ZKSarks \_formally.pdf
  -  zksarks.pdf

MPN networking test for more than half a year has been able to build a fast, directly connected and stable P2P network around the world through fewer nodes.



original dynamic keyless exchange algorithm (including double Elliptic Curve algorithm, packet transmission autonomous control algorithm, dynamic handshake algorithm, etc.) to solve the performance defects of TLS. It needs to exchange keys with each other in the process of using the security deficiency board and the protocol is not flexible enough, which is based on the introduction of the original dynamic keyless exchange algorithm (including double Elliptic Curve algorithm, packet transmission autonomous control algorithm, dynamic handshake algorithm, etc.). The original design principle of DN-TLS, which has been proved and tested by the team for a long time, has enabled both sides of the communication to transmit arbitrary data quickly, stably, securely and privately without exchanging keys and relying on relay.



### 4.3 SoFa Decentralized Name System

SoFa Decentralized Name System (SoFa DNS) is a decentralized DNS service designed for decentralized networks such as SoFa-Network. The Sofa DNS maintains a domain name -IP

mapping table in the whole network through block chain and the user locks the mapping relation of the specific domain name -IP through the Token and the private key. Also, it can change the mapping relation of the domain name -IP at any time. In this way, the traditional American-led DNS system can be switched to a decentralized DNS network to eliminate the threat of network hegemony and potential attacks. What's more, due to the need of Token to lock the mapping relationship between domain name and IP in the whole network, DNS can increase the cost of monopolizing a large number of domain names to a certain extent and reduce the cost of using domain name system by Internet users and Internet of things devices without the permission of domain name service providers.

#### **4.4 Proof of Packet**

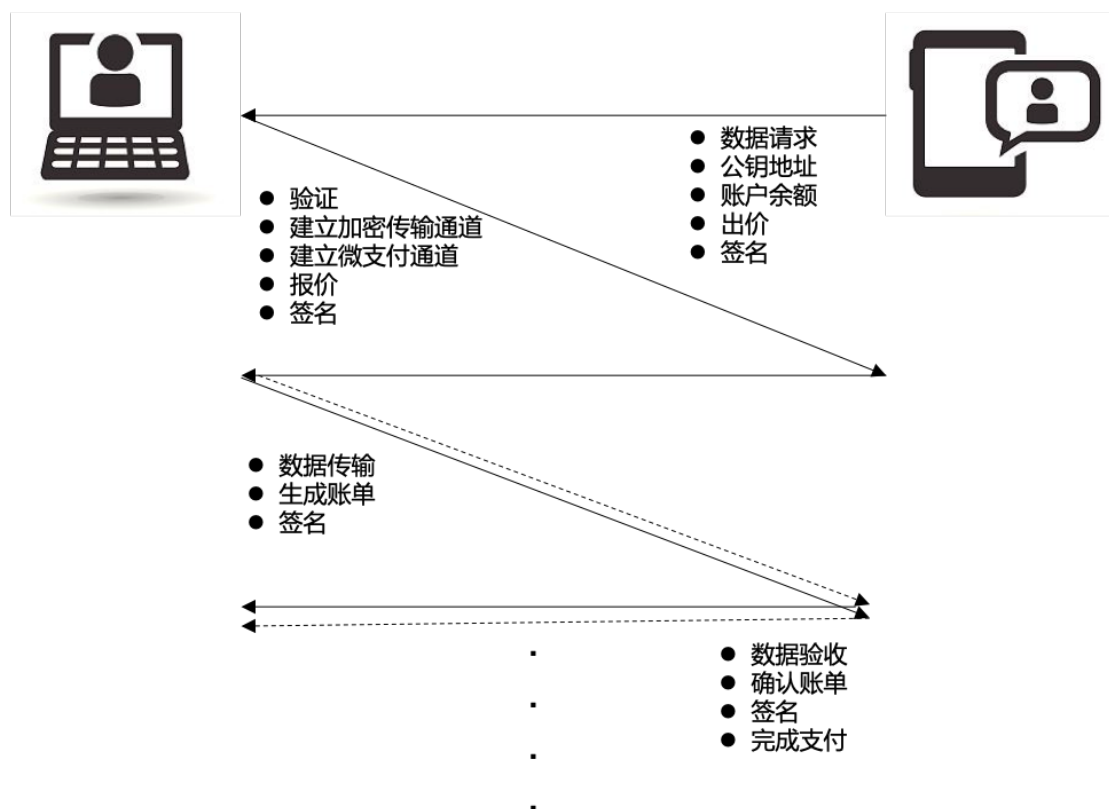
After the blockchain transformation of DNS system, SoFa-Network carries on the blockchain transformation to the data transmission of the bottom communication through Proof of Packet.

The existing supply model of Internet bottom communication service is provided by communication equipment service providers

in the unified laying of broadband optical fiber and other pipeline lines, the construction and maintenance of large switch gateways, and the construction and maintenance of mobile communication base stations. Then, some communication operators provide data communication services to enterprises and users. As mentioned at the beginning of this paper, due to the characteristics of high investment in Internet infrastructure construction, high technology content and long return cycle, the supply side of the communication market is monopolized by a few giants and the bargaining power of users is weak. And because of the underlying architecture and business paradigm of Internet centralization, the utilization of communication resources in the whole network is extremely uneven. The communication resources of backbone network are in short supply and congestion is expensive. The communication resources of edge network and terminal network are wasted by a lot of idle. The MPN constructed by SoFa-Network can effectively make use of a large number of idle communication resources in the edge and end networks and verify and settle the nodes that contribute the communication resources by the mechanism of PoP packet transmission proof.



When any two nodes on the MPN network connect and request communication, SoFa-Network can establish an exclusive encrypted transmission channel between the two nodes by DN-TLS and the PoP traffic proof algorithm can establish an exclusive micro-payment channel between the two nodes. When the data is transmitted in the encrypted transmission channel, the two nodes will dynamically count and sign the number and direction of the exchanged packets in real time. Statistical and signed traffic bills can be paid and verified quickly in real time through micro-payment channels.



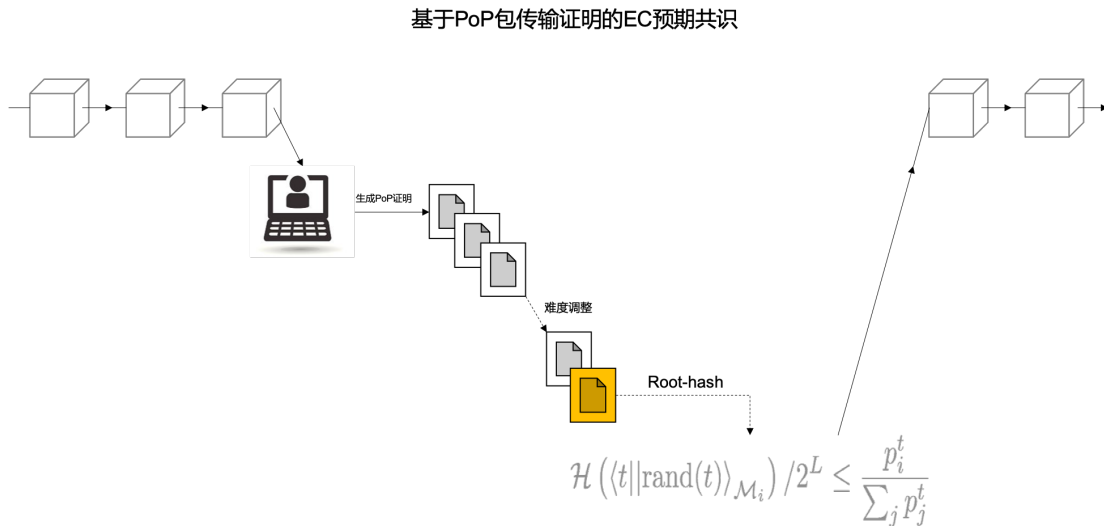
PoP packet transmission proves that it can be applied to any node connected to MPN network, including ordinary home routers, personal computers and mobile phones, data center servers, mobile communication base stations of communication operators, optical fiber devices, and even SpaceX communication satellites. PoP can also communicate and settle between two independent terminal devices without any other network connection through the wireless mesh network and synchronize the ledger data after any of the devices are connected to the network. This kind of efficient, non-tamper-proof, point-to-point communication and settlement method can effectively expand the boundary of the Internet. Let no man's land, deep-sea environment, and outer space be integrated into the integration of the global Internet.

## **4.5 Expected Consensus**

The Sofa-Network's block-chain accounting books section is a de-centralized and non-tamperable view of the entire network ledger through an expected consensus called the Connected Consensus (EC).

The Sofa-MPN network is a miner node, which continuously generates a PoP packet transmission certificate by contributing to

the service of its own communication resource for the user to provide data transmission. Then the PoP packet transmission held by the node of the current block is used to prove the participation in the election signed by the block. The whole process is as follows:



- 【1】 The miner continues to provide a data transfer service for the user;
- 【2】 The miner and the user double sign to confirm the PoP certificate;
- 【3】 According to the difficulty adjustment, the selected PoP generates the random number  $t$ ;
- 【4】 The miner participates in the secret leader election according to the random number  $t$  and the number proved by PoP.

- 【5】 The miner who was successfully elected the time secret leader of the block signed the confirmation block;
- 【6】 The whole network performs a new block campaign according to the block weight of the expected consensus.

## V. The economic model

### 5.1 Token Introduction

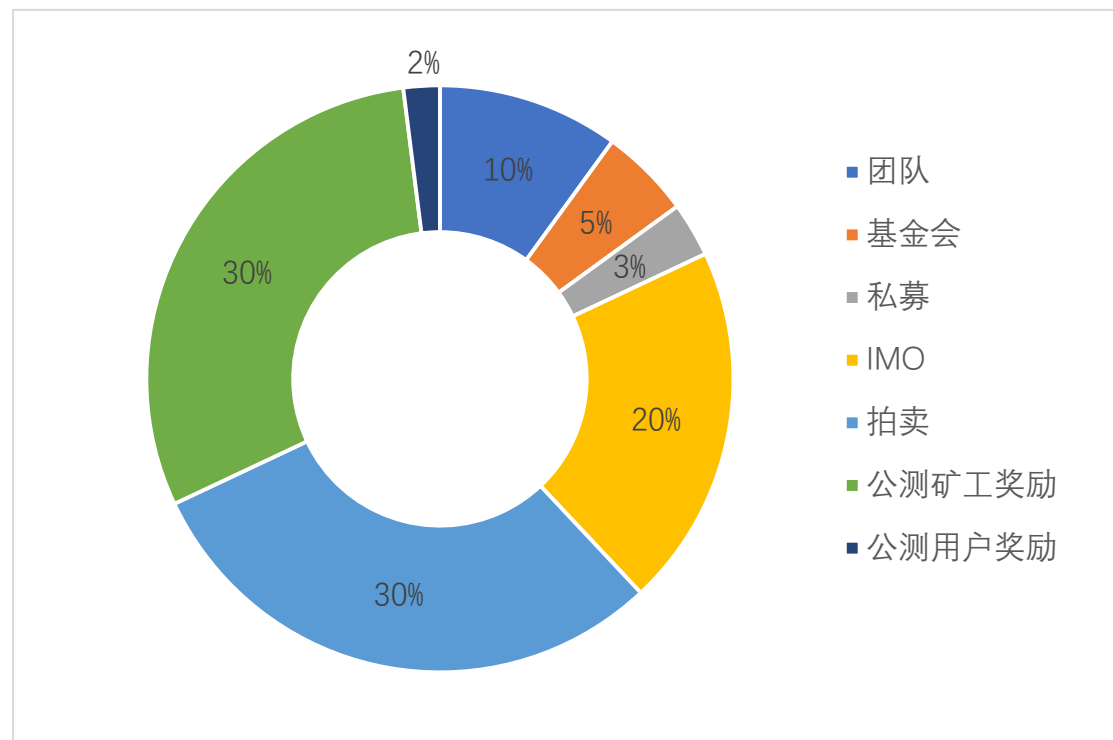
Token name: Phantom Matter

Token abbreviation: PHTM

Token total amount: 10billion. After the main network is launched, an additional 5% of the initial circulation will be issued each year as an incentive for out-of-block nodes.

Token attribute: The test period is ERC20Token and the end of the public test is 1:1 to the SoFa-Network main network token.

Token allocation:



## 5.2 IMO Plan

In order to accelerate the application of SoFa-Network to landing and accelerate the growth of the network, SoFa-Network will collect the first batch of super nodes and miners through IMO (for the first time for miners and super nodes) to build the network and distributed business ecology of SoFa-Network.

The users participating in IMO automatically became the first miners and super nodes of SoFa-Network. The miners and super nodes jointly started and formed the public test network of SoFa-Network.

The supernode can build an autonomous Dapp based on the Sofa-Network-based network and the SDK after the public test is started. Have the right to ownership and operations that the Dapp is fully autonomous.

IMO plans to issue 2 billion PHTM with up to 200 open super-node places. Also, institutions and individuals participating in IMO need to be approved by KYC. If the supernode of PHTM is obtained through IMO, it can apply to SoFaNetwork Foundation to repurchase PHTM at a specific price within one week after the PHTM is unlocked.

## **5.3 The Auction Mechanism**

Because SoFa-Network is already in the landing usable stage, the value of projects and Token will increase or decrease with the change of user size and the circulation number of Token will also promote or restrict the development of ecological applications. In order to adjust the supply circulation and pricing of Token according to the relationship between supply and demand, 3 billion PHTM will be issued by public auction.

The public auction is a Dutch auction, which is auctioned for 50 times every two weeks and 60 million PHTM is auctioned at a time. The PHTM issued by auction can be used in market circulation and network use immediately. In order to protect the interests of ecological users, ecological participants participating in the auction may apply to the SoFa-Network Foundation for a buyback of their PHTM at a specific price within the first week after six months of the auction time.

## **5.4 Public beta plan**

SoFa-Network is the network public test period from September 1, 2019 to August 31, 2021. During the network test period, SoFa-Network will release different stages of the network:

wormhole, Zhizi, and phantom to support more rich and different ecological applications. Different stages of SoFa-Network require a large number of nodes (miner and user). Ecological Dapp tests, uses, feedback and optimizes the performance and security of the network. The SoFa-Network Foundation will provide open-ended awards to miners and users during public testing. 3 billion PHTM will be used to reward miners during the public survey. 3 billion PHTM will be used to reward the miners over a 2-year period, depending on the number and contribution of the miners. In addition, the SoFa-Network Foundation will allocate 200 million PHTM to reward end users during the public test period. So that end users can not only use the network free of charge, but also get a certain reward, so as to accelerate the commercial landing of SoFa-Network.

## **5.5 Foundation Operation**

The SoFa-Network technology team hopes to focus on the development of network technologies and the rapid iteration of products, so the project foundation has adopted a model of entrusting third-party organizations to operate. Form the power structure of technical team, foundation and project community.



The SoFa-Network Foundation is responsible for the external cooperation of the project, community consultation, overall operation, ecological incubation, etc. The foundation also holds 500 million PHTMs, which can be adjusted and used according to the actual development needs of the project.

## VI. Project Team

To protect the privacy of the team members and the normal operation of the working life, the real name and the head portrait of members will not be disclosed to the outside, and only the resume of some members will be displayed.

### 6.1 Core Technical Team

#### **Sam/Funder**

The top ten network communication service providers of the world, senior network security engineers, senior network security experts, have more than 10 years of software development experience, and have a number of invention patents;

#### **Isaac/co-funder**

Network communication expert, Linux system expert, has served as technical director of many well-known Internet companies and network security companies. He has several invention patents.

#### **Ruaidhri/co-funder**

Senior big data risk control expert, network security expert, distributed system expert. 15 years software development experience and project management experience, former ZTE senior software research and development engineer, with several invention patents

## **6.2 Foundation**

### **Hung-Yi/President of Foundation**

Famous angel investor in blockchain, expert in block chain industry research, expert in communication industry, Internet observer

### **John/COO of the Foundation**

Early practitioners of blockchain, with many well-known block chain project operation experience and rich platform management experience

### **Jennifer/CMO of the Foundation**

Master of Media, Columbia University, Manager of Unilever Brand, Google big data Business BD,

### **Elaine/CFO of the Foundation**

Master of Financial Management, Project Manager of the Financial Audit of KPMG, and the enterprise's financial and audit experience for more than 5 years

## **6.3 Community**

SoFa-Network encourages community autonomy and select super nodes through the IMO program. Apply super nodes for fully autonomous community operation and community autonomy. At the same time, the SoFa-Network Foundation will also encourage

spontaneous user communities and miner communities through the early user Award Program and the miner Award Program. Through open community autonomy, SoFa-Network is committed to becoming a technical team, foundation, autonomous community tripartite governance of a self-organizing ecology.

All individuals and organizations can form their own SoFa-Network community at any time and anywhere and report it to the SoFa-Network Foundation. The report was not made out of permission. The community that has been reported will have the opportunity to receive various awards from the Foundation, including the Token, Community Welfare, offline parties, and so on.

The super node of SoFa-Network can rely on this node to establish a formal community. The super node has the power to develop and deploy independent Dapp/Dweb class applications on SoFa-Network and establish an independent user community.

During the Sofa-Network network public beta period, the Foundation will be responsible for the operational docking, support and support of the various communities. At the end of online public beta and before major network online, the

Foundation will convene community election meetings in all regions of the world to form a final community autonomy system.

## **VII. Risk Prompt**

### **7.1 Legislation risks**

The attitudes, policies and regulations of blockchain regulation and network review vary from country to country. SoFa-Netwokr network and all kinds of Dapp applications on it may have the risk of being prohibited and restricted by some national laws and regulations.

The SoFa-Network network is entirely formed and maintained by miners, super nodes, users and third-party developers. All miners, super nodes, users and third-party developers need to be aware of the requirements of the relevant laws and regulations in the host country in order to avoid losses due to legal risks. All illegal and criminal problems caused by improper use of the network shall be borne by the users themselves.

### **7.2 Market risks**

At present, the first stage of SoFa-Network has been developed and users can directly use all kinds of network-based Dapp applications during the public test period. Due to the

possibility of landing application, a large number of users have high expectations for this network. However, there are still large market risks in this network, such as the disappearance of market demand in some Dapp and the emergence of alternatives, resulting in a small number of users, which is not enough to support the value of the network or Dapp. All Sofa-Network users, miners and other ecological participants need to be careful to judge the market prospect and make the risk control. Inappropriate investment, mining, and operation may cause varying degrees of loss.

### **7.3 Attack Risk**

Even though SoFa-Network is committed to addressing privacy and security in the communication process, it still does not rule out the risk of cyber attacks from hackers or other organizations and governments. Attacks may lead to restrictions on network functionality, loss of Token assets, and so on.

### **7.4 Technology Risks**

SoFa-Network is an engineering implementation based on new network protocols, cryptography, consensus algorithms, etc. The

upgrade of network protocol, the breakthrough of cryptography technology, the potential vulnerability of consensus algorithm may affect the normal use of the network and the asset security of users.

## **7.5 Risk of using**

In the course of using the network, the user may have the condition that the key is lost and asset is lost due to the improper operation. In this case, a decentralized network is completely unable to help users recover their keys and assets. In particular, users of all networks must use the various functions, interfaces, and Dapp of the network correctly.