An Open and Universal Messaging Network

August 2019

Table of Content

1 Background

1.1 Origin

Internet is decentralized in essence. Though the centralized architecture of instant messaging serves people pretty well, we believe that the next competitive one would be an open and decentralized network. And instant messaging would not only serve social networking purpose, but also connect programs and things.

But how to identify users and things in such a network? How could we make this network more open so venders and service providers could join? Maybe we need to reinvent the instant messaging protocol. So that is what we are doing with DIM project.

1.2 Pain point

In the field of communications, Internet traffic hijacking by oligopoly and user privacy are particularly visible. Nowadays, users loses the right to choose their favor instant messaging apps and instant messaging oligarchs control all users' privacy.

What is more, relevant professional organizations predict that 2020 global connected devices will reach 10 billion units, including consumer products such as smart TVs, in-car entertainment systems, industrial applications that can predict plant maintenance needs or estimate the most efficient power distribution method for power plants. These applications can connect and interact on the same platform, creating opportunities for businesses to generate additional revenue. The rapid growth brought by the Internet of Things will have a profound impact on various industries in different countries, especially the communications industry, but there are also many problems.

1.2.1 IP address exhaustion

We’ ve been using IPv4 ever since RFC 791 was published in 1981. At the time, computers were big, expensive, and rare. IPv4 had provision for 4 billion IP addresses, which seemed like an enormous number compared to the number of computers. Unfortunately, IP addresses are not use consequently. There are gaps in the addressing. For example, a company might have an address space of 254 (2^8-2) addresses, and only use 25 of them. The remaining 229 are reserved for future expansion. Those addresses cannot be used by anybody else, because of the way networks route traffic. As we know, the pools of IPv4 addresses are close to depletion, but around 90% of the Internet is still only accessible via IPv4.

IPv4 is that, when the addresses were allocated, the internet was an American invention. IP addresses for the rest of the world are fragmented. A scheme was needed to allow addresses to be aggregated somewhat by geography so that the routing tables could be made smaller.

Yet another problem with IPv4, and this may sound surprising, is that it is hard to configure, and hard to change. This might not be apparent to you, because your router takes care of all of these details for you. But the problems for your ISP drives them nuts.

All of these problems went into the consideration of the next version of the Internet.

1.2.2 Security and privacy

Cybersecurity is a pertinent topic, and one which even artificial intelligence (AI) seeks to improve. With the Internet of Things, security stays at the forefront. IoT security risks derive from the fact that internet connectivity seeps into previously non-connected devices. As “dumb” devices become “smart,” securityu vulnerabilities exist. This might manifest as innocuous as a fridge being hacked to send out spam emails to hackers learning when you’ re home and away through monitoring smart devices to discover usage patterns. Overall, security is a massive pain point in the communication industry and even Internet of Things.

1.2.3 Cross-platform instant messaging

Nowadays, there are many instant messaging software on the market, but they cannot achieve cross-platform instant messaging. When users need to communicate, they need both parties to choose the same service provider to achieve instant messaging. In the final analysis, these instant messaging software are centralized and are not based on the same communication protocol. Therefore, the user can exchange messages only if both parties use the same instant messaging app. For example, A and B need to send messages to each other. A is a WhatsApp user, but not B, then B have to open a WhatsApp account. If not, B can not do instant messaging with A. It creates a problem that users have to download a variety of different instant messaging apps on their phone. In other words, all the user today loses their freedom to choose the communication service provider.

Although decentralized blockchain technology can partially solve the problem of cross-platform communication. However, main chains such as Bitcoin, Ethereum, and EOS, all of them have their own custom addresses under the existing blockchain system. It means users need to manage multiple different random addresses while using them. Another word, the problem is changed from user lost their rights to choose service provider to the need to select the same blockchain for instant messaging. So users still need to spend a certain amount of time to manage and learn to use new instant messaging app, which is not conducive to the development of cross-platform instant messaging.

Therefore, cross-platform instant messaging can only be realized if there is a decentralized instant messaging protocol and a unified identification of cross-chain account addresses

2 Related technology

DIMP (Decentralized Instant Messaging Protocol) is a decentralized instant messaging protocol designed by DIM team. Its birth based on a variety of mature technologies, and the review of these technologies and the appropriate hybrid application, benefit from the decentralized communication protocol design.

2.1 Blockchain

Blockchain technology is almost synonymous with decentralization technology, one of the reason is the special way of generating user accounts. In the traditional user account system, in order to ensure uniqueness, usually a center is uniformly generated and then distributed to the user; or the user applies for registration, then checks and processes, finally the center accepts and keeps it. It is conceivable that a unified and large centralized operation will lead to huge operational risks and costs in the future of the Internet of Things era; centralized operations by region or industry trigger the blockage of data flow. DIM are inspired by the account generation process of the blockchain. It is considered that the network terminal generates its own account and guarantees the uniqueness of its account in the whole network through mathematical methods. It is a very clever solution. Moving the steps of authentication from a centralized server to a terminal that requires communication is in line with today's advanced edge computing concepts.

2.2 DNS (Domain Name System)

DNS was born around 1985.It is an early product of the Internet. DNS is a distributed directory service that forms a hierarchical structure between domain name servers around the world, with root nodes in the United States. People can register in the DNS to register which domain names should access which IP addresses. This greatly facilitated the popularity of the Internet at that time, because people no longer need to remember the IP of four sets of numbers, but only need to input English words to access the website. We believe that unless the Internet-based TCP/IP architecture is rewritten, a mapping directory from name to IP address is required. Inspired by DNS, we can build a peer-to-peer, non-hierarchical directory service network to facilitate the promotion and application of decentralized communication protocols.

2.3 Smart Contract

Smart contract is a concept that emerge as the blockchain technology developing. Since the data on the blockchain is non-tamperable, the feature can be used not only to record transactions, but also to record the conventions between participants. Moreover, if these prior agreements can be saved programmatically, the smart contract can run faithfully at the right time. Smart contract makes it possible for collaboration between service providers without central organizers. Combined with the DNS service mentioned above, smart contracts can remove the root node in the middle of the directory service provider and achieve true decentralization. At the same time, well-designed smart contract can also support the economic cycle between service providers and users, enabling decentralized services to run in a long and orderly manner.

2.4 Email

Email was also born in the early days of the Internet, and it has been widely used until today. The e-mail system is open and multi-centered. It is very useful for decentralized communication protocol design. However, there has been no improvement in the confidentiality of messages, the reliability of message delivery between service providers and so on. All of these problems make our mailbox always filled with a lot of junk mail, and the existence of our account is very dependent on the service provider. The learning and review of the e-mail system architecture will benefit the decentralized communication protocol design.

2.5 Instant Messaging

Instant Messaging is already the mainstream of Internet communications today. From the desktop to the mobile, the products are endless, and have gradually evolved into a must-have feature in all Internet products.

3 Comparison of Open Source IM Protocols

In short, it is good to use alphanumeric addresses to identify end-users, so that we don’ t have to centralize the storage of usernames and passwords. But to keep the design simple and easy to scale, we also look into the architecture of email. DIMP (Decentralized Instant Messaging Protocol) is inspired by many existing protocols and internet technology, including blockchain, smart contract, email, DNS and etc.

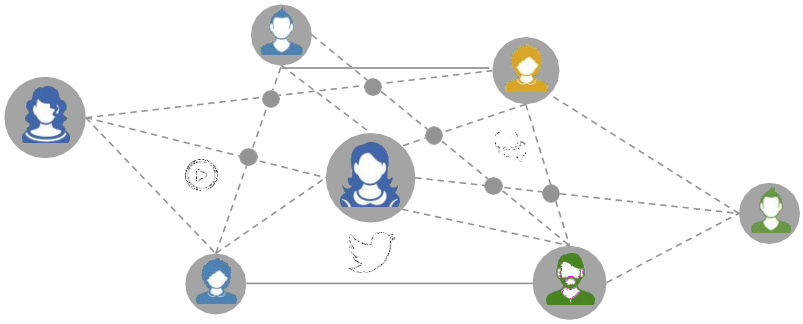
Node to Node Encrypt	End to End Encrypt	Public Board	Group Chat(1 to n)	Anti-Spam	Group Chat(n to n)	Instant Voice Call	Instant Video Call	FileSync	Decentralized
Yes	Yes	Yes	No	Weak	?	Yes	Yes	No	Optional
Yes	Optional	Yes	Client Side	No same standard	Optional	Yes	Yes	Yes	Optional
Yes	Yes	No	Yes	POW	Yes	No	No	No	Yes
Yes	Optional	No	Yes	Client Side	Yes	Yes	No	Yes	No
Yes	Yes	No	Yes	Yes	Yes	No	No	No	Yes
Yes	Yes	No	Yes	Client Side	Yes	Yes	Yes	Yes	No
Yes	Yes	No	Yes	Client Side	Yes	No	No	No	Optional

Compared with the extensive application of SMTP in the Email era, communication between server nodes has progressed, that is, attention to confidentiality. But end-to-end encryption is still an option. The protocol that emphasizes end-to-end encryption cannot implement the bulletin board function because the message needs to be clear to the recipient and even encrypted with the recipient's public key. This naturally increases the complexity of the bulk and group chat features. But the biggest challenge is in the anti-spam function. After all, if only the recipient can decrypt and read the information, the server will not be able to intercept the spam when forwarding the information. The existence of spam threatens the performance of the entire network.

Support for real-time voice/video communications is a test of protocol scalability. Traditional IM applications in most cases process and send and receive information asynchronously, and the information that does not reach the recipient client needs to be cached. But real-time voice/video communication is synchronous, unlike the asynchronous information processing mechanism. The file synchronization function is similar, but this function has a certain tolerance for time delay and is mainly applied in collaborative scenarios.

It's not hard to find that protocols that use phone numbers as user IDs inevitably require a centralized deployment. Decentralized deployment, or multi-centered deployment, is an indicator of openness to the agreement. In other words, the protocol that supports decentralized deployment will allow multiple vendors to jointly develop and provide product and communication services from the server

to the client.



According to the arrangement of the initial agreements, you can see the changes in the design ideas:

SIP is an early industry standard, and XMPP is an open protocol advocated by Google when it comes to launching IM products. Both use a format similar to an email address to identify the user. They are more focused on solving communication problems, so they are lacking in social functions such as group functions;

With the emergence and development of Bitcoin, the protocol of bitmessage was born. The protocol uses the string address common in blockchains to identify users and uses POW (workload proof) to prevent spam from spreading in the communication network. POW greatly reduces communication efficiency and limits the scalability of the protocol;

Telegram's MTProto protocol undoubtedly found a breakthrough in the market for encryption features and balanced product ease of use. The only thing it sacrifices is the decentralization feature. The following year, Signal also launched a similar agreement;

In terms of emphasizing confidentiality, there is another alternative that relies on darknet and onion routing systems. User IDs are even dynamic. Ricochet is the representative of this type. Such agreements will undoubtedly inhibit the transmission of spam, but the scalability is relatively poor, and the resulting communication products are more difficult to use.

4 DIM Technical details

4.1 DIMP (Decentralized Instant Messaging Protocol)

DIMP (Decentralized Instant Messaging Protocol) , which was born at the end of 2018, is a decentralized instant messaging protocol. It can be used not only as a basis for human-to-human social products, but also as a cross-blockchain, cross-enterprise data exchange tool, and even applied to the underlying layer of smart device networking communications. Our vision is to make DIMP a communications engine that drives the Internet of Things.

DIMP features：

- **Decentralized:** The user ID format is compatible with Bitcoin, Ethereum, EOS and other mainstream blockchain account addresses.
- **Open:** Adapt to the changes in the number of service providers and the regulatory requirements of communication services in different countries.
- **Safe:** All types of messages are given point-to-point encryption protection, and intermediate nodes cannot be tampered with.
- **Adaptable:** Support high concurrency and low latency. The bottleneck depends only on the network environment and the service provider.

Basically, DIMP (Decentralized Instant Messaging Protocol) has three key components to work.

- Addresses Generation
- End-to-end Encrypted Messaging
- Address Naming Service

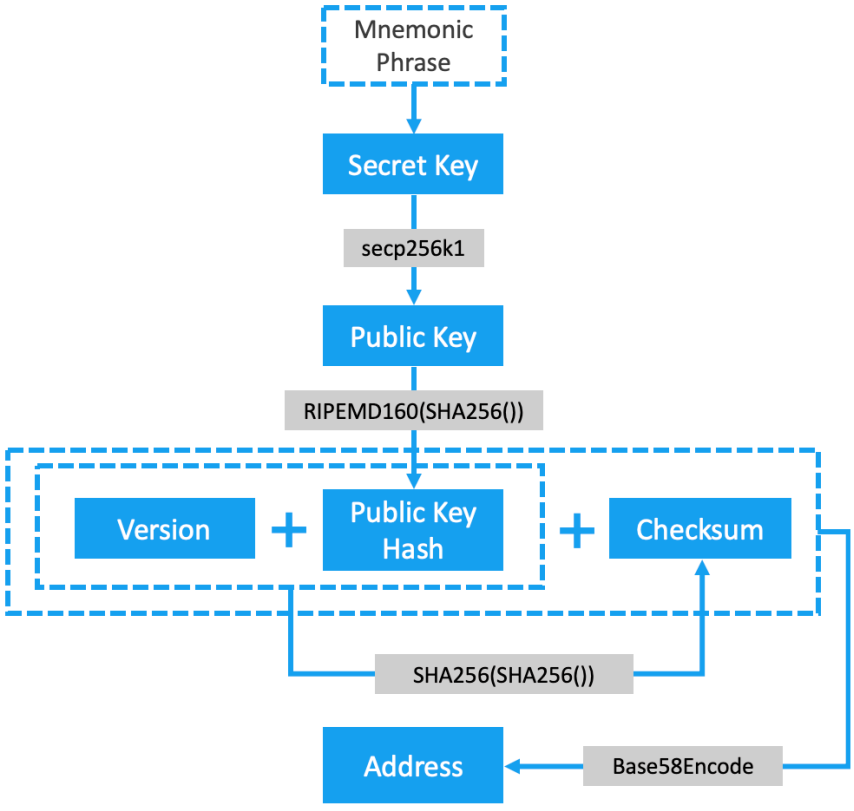
4.2 Addresses Generation

The examples of end-user ID are shown below, which are in the same format of bitcoin or Ethereum. We think that identifying end-users with this kind of addresses is the good practice in a decentralized system.

1FmWXNJT3jVKaHBQs2gAs6PLGVWx1zPPHf

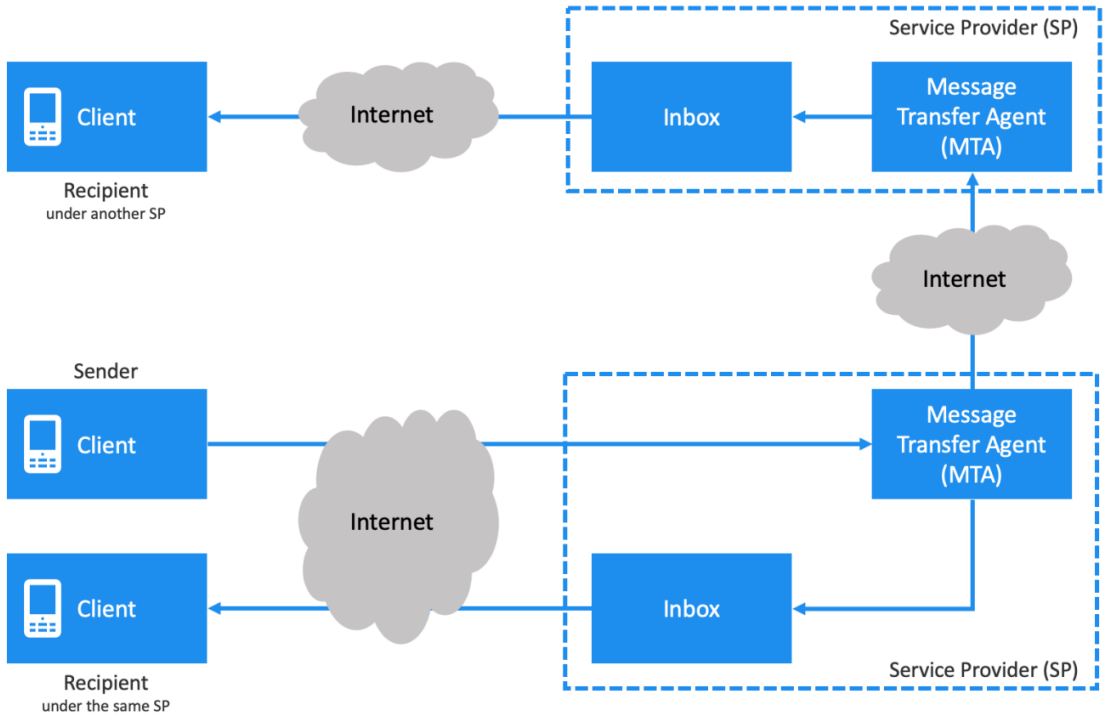
0xd91c747b4a76B8013Aa336Cbc52FD95a7a9BD3D9

The mechanism of generation is illustrated below.

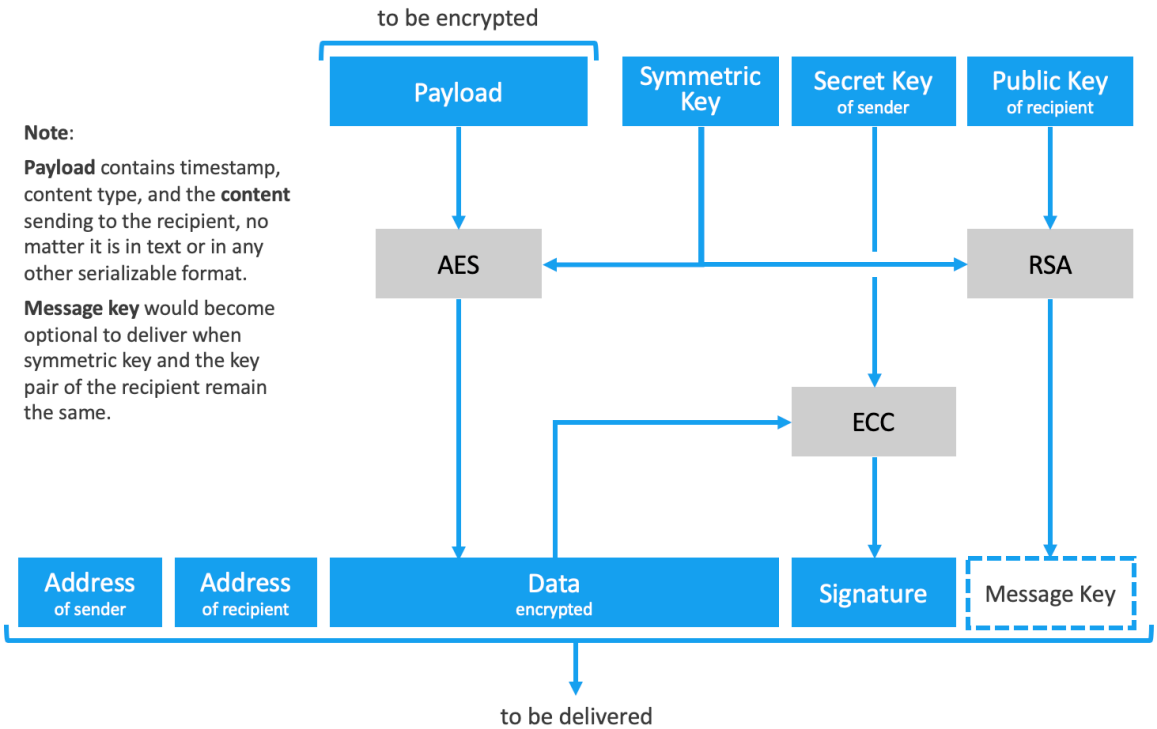


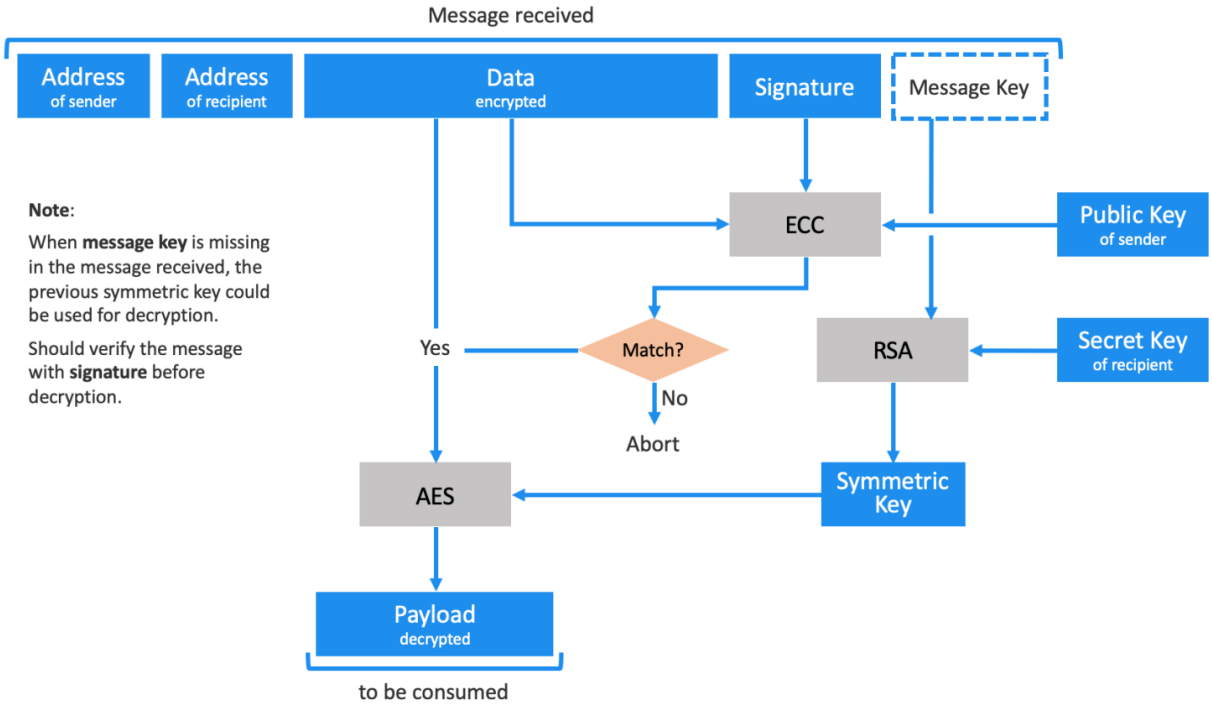
4.3 End-to-end Encrypted Messaging

The route is similar to what an email is delivered, and it is shown as below:



The SP provides servers or nodes to relay messages. And the encryption process is illustrated below, followed by the diagram of decryption process.





4.4 Address Naming Service (ANS)

ANS is something similar to DNS of internet. It provides a directory so that SPs could find each other, and the user addresses could have the meaningful destinations. It is implemented as a blockchain, so SPs become the nodes of the decentralized network and would gain incentives to maintain ANS.

4.4.1 Token system

ANS is the key to the normal operation of a DIMP network. Based on this, we issue DIM Token (code DIMT) as proof of equity for this network operation. Any SP must hold a certain amount of DIMT to provide services. The SP takes turns to add records in the ANS; using the POS type consensus algorithm, a DIMT reward for the SP responsible for verifying the new record.

4.4.2 Name Registration Service

In the general scenario, the end user is free to use the DIMP network. Since the user address is a string of English letters and numbers, the user cannot name it himself, which is very difficult to propagate and retrieve. Therefore, based on ANS, we have added a username registration service. On a first-come, first-served basis, users can customize the name and map it to their DIMP address. This service requires the user to pay a certain amount of DIMT per year as a registration fee.

ANS will open the query interface to the outside world and have the opportunity to apply the username-to-address mapping to scenarios outside the DIMP network

4.4.3 Network Maintenance

The DIMT's way of circulation fully demonstrates the autonomy of the DIMP network. In essence, the end user pays the operating cost to the service provider. The more network users, the higher the service provider's revenue. Users are free to choose SP; and SP can innovate, attract users and complete DIMP.

5 Applications

DIMP will be the communications foundation for the decentralized ecosystem. Communication between people, communication between people and things, and even communication between things and things can be decentralized, traceable, and non-tamperable based on blockchain technology under the DIMP, proceed safely and efficiently.

Any existing application, as long as there is communication needs, such as chat, file transfer, remote control, etc., can be implanted on the original basis of DIMP, upgrade communication functions, without changing the original features of the program, to overcome The shortcomings of the original application centralization, so that all things are interconnected, breaking the communication barrier between similar but different company software. Users can use the communication software application with confidence, get rid of the communication barrier between the applications, and truly "free travel" in the Internet world; the user group breaks the communication barrier between the applications, the user groups are common, and the enterprise can get rid of Insufficient user groups create concerns about the inability to form a communication ecosystem, and exploit the characteristics of the services provided by the company itself to develop features, such as the existing centralized chat software industry.

Therefore, in the new ecosystem based on DIMP as the communication, whether it is communication between people, communication between people and things, communication between things and things, can communicate and exchange value more safely. work together.

5.1 Social Communication

5.1.1 Cross-platform instant messaging

Based on the characteristics of decentralization, security and reliability, DIMP will become the basic technology protocol for new instant messaging applications, setting off a new generation of communication methods – cross-platform instant messaging.

Almost all the existing instant messaging apps on the market are centralized. Therefore, there are communication barriers between instant messaging apps. That

is to say, most users have to download multiple different instants in order to meet the inevitable needs of life and work.

Now, users can select the instant messaging platform according to their own preferences under setting up the instant messaging app based on the DIMP. We take an example that A is a WhatsApp user and B is a Telegram user. In the traditional instant messaging system, they cannot communicate with each other. However, if both WhatsApp and Telegram are moved and implanted in DIMP, instant messaging between A and B can be done without same app or service provider.

In order to facilitate user learning, DIM team developed a DIMP-based communication app named DIM CHAT as an sample application on DIMP. In the future, more individuals and communications companies will begin to realize the advantages and significance of decentralized instant messaging protocols. Then the present instant messaging apps is gradually going to move to DIMP. By then, a new generation of communication methods - cross-platform instant messaging will be a trillion-level application needs, serving billions of users around the world.

5.1.2 Cross-chain name service

Bitcoin, Ethereum, EOS and other mainstream blockchains all have their own custom account addresses. Users need to manage multiple different random account addresses at the same time. In other words, users need to select the same blockchain account address form in order to achieve instant messaging. In addition, in the general scenario, the end user is free to use the DIMP network. Since the user address is a string of English letters and numbers, the user cannot name it himself, which is very difficult to propagate and retrieve.

DIM's name service (aka. ANS) solves these problems. Based on ANS, DIM adds a username registration service. On a first-come, first-served basis, users can customize their names and map them to their own DIMP addresses for cross-chain instant messaging, greatly reducing the cost and barriers to decentralized instant messaging.

Today, as the number of Internet information explodes, we are also growing in social circles. There are more and more contacts around us. At the same time, mobile phones are replaced and mobile phone numbers are frequently changed. If

data migration is insufficient, it may cause us to lose. The contact information of the other party, or the contact information of the other party has changed, and it is also a problem we often encounter. Many of the current contacts save the means of migration, such as the SIM card's own storage function, cloud disk storage function, but in any case this is a centralized storage system, data privacy security can not be well protected.

In the decentralized ecosystem based on DIMP construction, the above problems are well solved. The user's contact information is no longer just a string of digital accounts, but an address based on decentralized technology. Users are bound to their own account name and blockchain address at the SP point. The establishment of contacts is based on a DIMP distributed network. Suppose a social DAPP is closed, or the mobile phone is lost. Users only need to select any DIMP-enabled DAPP to import their own account information and related blockchain address information, and then log in to their own decentralized account and import them at any time. Contact information of past contacts, continue to communicate with contacts, send and receive information, to avoid the loss of contacts.

5.2 Digital Asset Management

5.2.1 Decentralized Wallet

Blockchain wallet key management tool, which only contains the key instead of the exact one of the tokens; the wallet contains the pair of private and public keys, and the user signs the transaction with the private key, thus proving that the user owns the transaction The output rights; and the output transaction information is stored in the blockchain. It rules the user's money, manages keys and addresses, tracks account balances, and creates transactions and signatures. Provides basic financial functions such as creation of wallet addresses, encrypted digital currency transfers, and query of transaction history for each wallet address.

DIMP can also be used to build a decentralized wallet. With DIM cross-chain technology, you can build a DIM cross-chain wallet that stores a wide range of digital currencies such as DIMT, Bitcoin, ETH, EOS, USDT and more. At the same time, the concept of cross-chain wallet can also be grafted to other DIMP-based DApps through DIM technology, such as social DApp, food delivery DApp, etc., to save, purchase, trade and so on in the DIMP-based ecosystem.

Suppose an enterprise needs to develop an innovative point-to-point sales platform reference program that involves the configuration of payment functions. In an

ecosystem built on DIM-based technology, this part of the work becomes more convenient and faster. Users can import/export their own decentralized wallet in DApp for the first payment. Therefore, all trading behaviors are recorded on the blockchain. Transaction records are traceable and non-tamperable, ensuring efficient trading practices.

5.2.1 Decentralized Exchange

There are two types of digital asset exchanges on the market today. One is a centralized digital asset exchange, and the other is a decentralized digital asset exchange. The former accounts for the vast majority.

Centralized exchange: A platform or application that allows traders to buy or sell cryptocurrencies using fiat or other cryptocurrencies. It is the market for token trading. The user deposits the money directly into the exchange, and the exchange stores the funds as a wallet until the order is generated. Exchanges keep their systems under the chain, which means that these transactions are not recorded by the blockchain. Once the order is generated, the exchange will match the buy and sell orders in real time. In this case, the key point is that when you deposit funds or trade on such an exchange, you do not know the private key of the cryptocurrency. Although storing your encrypted assets in a centralized security has all the security, it also has fundamental risks, such as the collapse of the exchange or large-scale hacking.

Decentralized exchanges: The goal of a decentralized exchange is to create a "person-to-person" market directly on the blockchain. Funds are not delivered to a single exchange or wallet owned by a single platform or institution: instead, orders and transactions take place on the blockchain. As a result, there is no middleman cost, assets are not affected by hacking, and users actually have control over assets. Although most security issues are resolved, there may be inconveniences due to lack of users, lack of ability to support cross-chain trading orders, and so on.

The introduction of DIM decentralized instant messaging protocol will greatly offset the shortcomings of decentralized exchanges. The DIM Decentralized Instant Messaging Protocol is an infrastructure or platform that allows anyone to build their own services on top of them to run decentralized applications. A "protocol" is a conduit that carries decentralized applications. On decentralized exchanges, open agreements are designed to allow all established projects to interact to create a shared liquidity for the exchange; at the same time, DIMP supports cross-chain communication capabilities for decentralized exchanges. The function of cross-

chain trading orders greatly facilitates. Users only need to import their own decentralized digital asset wallet in DIMP-based decentralized exchanges, which can be extremely convenient for point-to-point cross-chain transactions, without third-party interference, from hacker attacks, transactions. The liquidity is also guaranteed.

The DIMP-based decentralized digital asset exchange can truly decentralize, cross-chain transactions, be free from hacker attacks, and have high liquidity guarantees.

5.3 IoT

The Internet of Things is actually a network of devices that do not require any interference with each other. The devices themselves create, modify, delete, send and receive data with each other and use that data to make decisions. The application prospects of the Internet of Things are very broad, such as in the smart home, transportation, and industrial production fields. However, in the long-term development and evolution process, there are a lot of problems during the development of the Internet of Things.

DIMP is a decentralized instant messaging protocol based on blockchain technology. With the characteristics of peer-to-peer, open and transparent, secure communication, difficult to tamper with and multi-party consensus, it will have an important impact on the Internet of Things: multi-center, weak center The characteristics of the system will reduce the high operation and maintenance cost of the centralized architecture; the characteristics of information encryption and secure communication will help protect privacy, protect the Internet of Things communication, make the Internet of Things more secure, stable and reliable; identity rights management and multi-party Consensus helps identify illegal nodes, prevents malicious nodes from accessing and doing evil in a timely manner; generates addresses based on the principle of asymmetric encryption, only 2^160 for bitcoin types, and almost zero for the same private key. It can guarantee the uniqueness of the whole network and better solve the problem of depletion of IP addresses; relying on the chain structure can help to build evidence-proof traceable electronic evidence; the characteristics of distributed architecture and subject equivalence help Breaking through the existing information islands of the Internet of Things, promoting horizontal flow of information and multi-party collaboration.

Therefore, DIMP can be applied in the field of Internet of Things in the future, which

can effectively solve the pain point of the development of the Internet of Things and become the communication engine that drives the Internet of Everything.

6 Roadmap

Nov 2018 DIMP Technical White Paper Released

Feb 2019 IOS test version launch

Apr 2019 Group chat function is completed

Q3 2019 Wallet release

Q3 2019 Deploy the initial node of the distributed network

Q4 2019 Launch Objective-C、Java、Python SDK

Q4 2019 Publish standard server installation

Q1 2020 Launch TestNet

Q1 2020 Open service

provider application

Q2 2020 Launch MainNet

Q3 2020 Release

micronode standard

Q4 2020 Release IoT application standards