DECENTRALIZED INSTANT MESSAGING NETWORK

WHITE PAPER

V1.0

2018.11.18

TokTok Network

CONTENTS

EXECUTIVE SUMMARY

Slogan: A new generation of large-scale instant messaging network supported by blockchain.

Project Description: The key feature of “TokTok” is a kind of "WeChat", the difference is that it is decentralized, fully internationalized, without any state control or monitoring, with end to end encryption security. The goal is to make users around the world follow us, because today " WeChat " has fully proved its own product design, user experience, and its great value in the Chinese community.

Roadmap to success: The project is simple in positioning, product design and market have been fully verified, and the market risk is small. The core technical team member was "WeChat" core patented inventor, technical risk is smaller.

Core advantages:

- Built with distributed technology, secure, reliable, fully protecting user’ privacy and digital asset security
- Clear target market, product positioning, there is value to meet the needs of influencers’ value exchange
- The market potential is huge, and the demand is urgent. At present, there are few similar products, and the functions of the substitute products are limited.

- The market entry point is clear, the market growth strategy is feasible, and it is worth looking forward to becoming a unicorn project.
- Digital wallet and DApp as a plug implanted, to meet the needs of the market
- Mature technical solutions, strong team, low investment, quick results

The mobile instant messaging platform has culminated since 2010 and has been through 8 years. Whether it is a huge amount of financing for bullet text messages, or the ICO of Status.im and
Telegram has been enthusiastically sought after by the currency, it is time to say that the time has come to change the fundamental platform of mobile instant messaging.

1 THE PROBLEM

Since 2010, KIK Messenger set off a wave of mobile instant messaging mode change, micro letter, WhatsApp, Facebook Messenger, Line, repre sented by mobile IM tool, and gradually developed into a force at the core leading the market, changing the billions of Internet life. Such tools, on the one hand, have changed the way people communicate, and on the other hand have changed the way socializes socialize. With the surge in import users, relations of production, people’ s economic activity has gradually done through instant messaging.

A typical product is the WeChat. Since the introduction of the WeChat Wallet, now it becomes payment method for many online websites and mobile applications, but also offline stores. Trends prove that social tools, from the original popular social media, have gradually deepened into an economic platform that connects users and businesses, and carries user consumption activities and trading activities. This development trend has just begun, and this trend is constantly evolving and upgrading.

" WeChat ", user-centered, imported mobile address book and social relationship, replaced the traditional mobile communication method, implanted the timeline social status system, joined the mobile payment method, and established the Official Account platform, which is fast Become the core carrier of people's communication, social

and economic activities. However, " WeChat " can only serve as the pinnacle of the information Internet era.

1.1 Security and Privacy Challenges

As social media evolved into a social economy platform for value exchange, we realized that many deadly problems with traditional social platforms were not resolved. First, the user's information security and communication privacy are not effectively protected. Secondly, the user circle of friends formed on social media, avatars of these intangible assets, and did not get effective protection, instant messaging operator can delete such content at any time. Again, users with a large amount of data, including contacts, social relationships and share content, communications operators seek a variety of interests, and therefore does not bring any financial reward to the user. Finally, as a hub of economic activity and value exchange, the form of economic exchange activities between users is limited, and the issue of trust cannot be effectively solved.

1.2 Impediment of Trust

As the Internet develops into a new phase of value Internet, the era urgently calls for a central platform for value exchange. Based on this platform, each user can become a participating unit of value Internet and enjoy the safe, reliable and efficient life of the digital economy. Unfortunately, the traditional center-based technology architecture built mobile instant messaging platform, cannot bear

this mission. Traditionally IM platform, users do not have ownership to their accounts, have no freedom of speech. It is difficult for users to participate in full, intelligent value exchange activities.

1.3 Bottleneck for Value Exchanges

With the continuous development of Internet technology, the value of super-individuals as content creation and dissemination on the Internet is becoming more and more significant. Influencers and opinion leaders not only spread the UGC, but also spread the industry knowledge and become an important force influencing consumer decision-making. The popularity of mobile terminals, social networks and payment channels has created enough conditions for communication and value communication between users and users. We have noticed that the knowledge payment market is booming. However, the instant messaging tool platform does not provide sufficient support for knowledge exchange services and does not provide support for the simplest functions such as making payment to join groups. For more value exchange requirements, due to the limitations of the platform itself, it does not provide enough support.

2 TOKTOK NETWORK SOLUTIONS

TokTok 's product solutions include three major parts: the client product TokTokApp , the online platform TokTok Network , and the TokTok Official Accountplatform . TokTok Network network platform as the basis, bearing account

management, user communication, data storage, the three major core-basedenergy. Ordinary individuals connected by TokTok App to TokTok Network, use the network resources and services, enterprises, groups of users TokTok number of public information dissemination platform maintenance in TokTok Network.

2.1 TokTok App

TokTok App, based on distributed technology to build, user accounts, data and digital assets owned by the user to create a safe, social environment, freedom of speech, and on this basis, people can participate in a variety of value exchange Activities.

The basic functions of the TokTok App

Multimodal message	Circle of friends	File sharing
Encrypted voice call	Encrypted group chat	Live video
Encrypted video call	Cross-platform	Multi-language support

TokTok App's features

Local account	End-to-end encryption	Offline message
Decentralized cloud storage	Ready to burn	Automatic lock screen
Smart group chat	Digital wallet	Token incentive

Screen capture reminder Offline sync IP confusion

Local Identity. The TOKTOK network generates a unique private key and corresponding account system for each participant. It uses a mechanism like CIVIC and UPORT to store the user's private data locally. More data is stored in the IPFS cloud in encrypted form, eliminating password leakage and exposure of user data security issues. In addition to the local account system, it also includes the operation of social relationships, which translates the traditional user relationship into the relationship of the user in the system by matching the user's relationship resources.

Offline sync. If the internet connection is lost, the client software will transfer the data via Bluetooth or W IFI to ensure that the user is still available. If the internet connection is restored, the data is synchronized via the Tor network.

Global communications. Since the TOKTOK network is a distributed network and its node branches are all over the world, the traditional firewall cannot prevent users from using the network to send messages by prohibiting the server IP.

2.2 TokTok Network Introduction

Traditional mobile instant messaging tool, there is a privacy protection is poor, poor security, freedom of expression and the user cannot get a lot of data ownership issues are fully guaranteed, is the center of technical architecture and business model of the decision. With

traditional centralized technology architectures and operational models, these issues cannot be fundamentally addressed. Because of the centralized mode, the storage and computing resources of all servers are borne by the operators, so operators are bound to distribute these costs to users in disguise. Government due to the centralized management, operators must be to the jurisdiction of the responsible, so that data stored in the cloud will inevitably be subject to government censorship, not government welcomes the account is bound to be blocked, the Government considered unsuitable remarks bound Will be deleted. Because operators provide free resources for users to use, users have lost the value of their own claims to provide data creation.

Science and technology are the primary productive forces. Blockchain technology, and the distributed storage and computing, encryption and decryption, shared ledger and smart contract technology used by it, can fundamentally solve many problems of traditional instant messaging platforms. The traditional instant messaging platform relies on the cloud's central server to forward and store messages, while the TokTok network utilizes the decentralized DHT network distributed architecture. There is no central server at all, only some relay nodes, these nodes only serve as bootstrap. Function, both sides of the chat are completely P2P, end-to-end encryption. TOKTOK NETWORK uses key technology, the user's account as a network participation unit, except for the user itself, no one can delete. Users of digital assets, operators cannot deprive. The social platform cannot perform business intelligence analysis and advertising based on user data without user authorization. Users have the right to freedom of

communication. Users of digital assets managed by the users themselves, account password leak problem no longer occurs. Based on this, users and users carry out various rich and colorful economic activities. The trust problem is solved by blockchain technology, and the books are clearly visible in the blockchain.

2.3 TokTok OFFICIAL ACCOUNTS Platform

TokTok public platform, sub-publishing content management (CMS) and subscriber management two modules.

3 DISTRIBUTED MESSAGING NETWORK (DRN)

Unlike centralized IMs such as MSN, WeChat, Telegram , and WhatsApp, TokTok uses a distributed network architecture . The traditional decentralized IM is divided into two types. One is a self-hosted service like IRC, Rocket Chat, and Matter Most. Users between different servers cannot communicate. One is to use a federated service similar to the mail system, such as XMPP. And Matrix. TokTok is more advanced, similar to GNU Ring. P2P , the server itself is only used to help users discover other users. Once the user finds the other party to the communication, the communication data is transferred directly between the communicating parties without going through the server.

In the TokTok network, the servers used to help users discover other users are also decentralized. These servers are built on the relay nodes of the network. As an example of a service for making a VoIP call, the system generally requires an Agent server. In the TokTok network, the Agent server also exists in the decentralized relay node. After a UA logs in, its IP and port information is recorded in a distributed hash table by hashing. If a node goes offline, it does not affect the addressing of the UA, nor does it affect the established P2P communication process.

As a basic node of the chat service, the relay node is convenient for establishing instant-to-point instant communication between users. Each relay node contains three modules: routing table, message queue, connection adapter, and backup.

When the user registers and uses the TokTok App for the first time, when the user's basic information is verified, a new node is created and added to the routing table of the other node. If the recipient is online, the message is passed directly over TCP. If the recipient is offline, the message is sent to the nearest neighbor, and when the recipient goes online, it can be quickly forwarded.

4 DISTRIBUTED STORAGE NETWORK(DSN)

Throughout the chat system, in addition to the relay node, the storage system there is user information. The TokTok network uses a distributed file storage system, and each user's data is stored in multiple nodes in the form of encrypted fragments. On the one hand the system provides storage, on the other hand provide temporary storage. In the case where the client is offline, the content needs to be cached by the node. Examples of multi-condition to ensure that each terminal can obtain the message, and the message is synchronized in time. In addition to the regular file storage, the session data in each session is encrypted according to the session ID and the user's private key, and then the encrypted file is stored in fragments on multiple servers, only the participants of the session. This data can be synthesized and decrypted.

5 END-TO-END ENCRYPTION(E2EE) SECURITY

End-to-end encryption for instant messaging has evolved to the third generation, and the system uses the latest encryption technology. The earliest OTR uses key exchange to achieve forward and backward security and achieves integrity through a symmetric authentication-based message authentication code (MAC)non- digital signature; SCIMP uses a hash iteration-based approach to generate an encryption key to achieve forward Safety. TokTok network draws on the Open Whisper Systems agreement to combine the two key generation mode, dual ratchet (Double Ratchet) algorithm, enhanced authentication and encryption of communications RTP and RTCP messages to ensure communication between the parties, group chat, can Encrypted transmission of messages, pictures, audio, video and other files guaranteed.

In the present system, the dual ratchet algorithm is used for communication parties to exchange encrypted messages based on shared key exchange. The communication parties are based on the extended Huffman (Triple Diffie-Hellman, X3 DH) KEY negotiate a shared key exchange protocol, and then sends the encrypted message can be received using a dual ratchet algorithm. Each one pair of ratchet message derives the new key, so that the key cannot be calculated from the new old key obtained. The two parties will also attach the Diffie-Hellman public key value to the message. The results of the Diffie-Hellman calculations will be mixed into the derived key so that the new key cannot be calculated

from the old key. Even if the key of a message is leaked, the hacker cannot decrypt the previous message and the subsequent message, so it has forward and backward security.

6 TOKTOK BLOCKCHAIN

The TokTok blockchain is used to track the exchange of TokTok network consensus values. Unlike the Telegram public chain, the Telegram blockchain allows developers to develop based on Telegram's public chain, requiring Turing completeness and high performance. The TokTok block chain is only as TokTok network services, rather than TokTok web developer services. In the future, after the TokTok network grows, developers can develop smart contracts based on other public chains, and their programs will be used by the TokTok network. The TokTok network will have built-in intermediate layers of various public chains to support the use of other public-chain smart contract programs on the TokTok network. The design of the TokTok public chain, in terms of positioning, is more like a connector that diverts traffic and load to other public chains.

TokTok Chain is a blockchain underlying technology solution based on primary sidechain and fragmentation technology. It is a decentralized, high performance, scalable superblockchain that will enable transaction processing of millions of chains per second. Capabilities (1,000,000 + TPS), and a query processing capacity of 1 billion per second (1,000,000,000 + QPS). In order to balance the security and efficiency of the transaction, the main chain adopts the VDPOS consensus algorithm (created variable proxy equity proof algorithm), and the side chain adopts the P BFT consensus algorithm. Ensure that each chain can support thousands to tens of thousands of transaction requests, as well as security guarantees.

The consensus mechanism is the core technical point in the blockchain. A process in which a multi-party node agrees on data, behavior, or process through interaction between nodes under a preset rule is called consensus. The consensus mechanism refers to the algorithms, protocols, and rules that define the consensus process. The VDPOS algorithm, which is highly efficient and prevents network congestion, prevents the network from being congested. It can achieve the second-level confirmation and can solve the problem of performance and energy consumption.

7 USE CASES

In addition to
traditional "WeChat" application scenario, TokTok addition tothe safety communication, privacy protection, and the distributed data storage multimodal chat function and use of these scenarios, the use of the block chain technology, application scenarios with more colorful.

	Description
Forecast market	Friends can place a bet to predict whether the Shenhua team will win the football match tomorrow, and the winning party will automatically receive a red envelope reward of 50 USD. This is a very typical scene, and it is often done between friends, but traditional mobile IM does not support it. With smart contract technology, such a scenario can be very easy to implement. The blockchain adopts ORACLE technology, which will automatically obtain the results of the game to execute the red envelope process, which is fair and accurate.
Group management	The group owner can set the rules. Anyone who enters the group needs to pay 100 USD as a deposit. In the group, if the advertisement is sent, the 100-usd deposit will be deducted immediately. If the group is dissolved, the 100-usd deposit will be refunded automatically. Through blockchain technology, group rules can be flexible and automated, all managed automatically through smart contracts .

Content incentive	Any content that gets more forwarding and support in the circle of friends can accumulate a certain reputation value and can obtain certain platform rewards based on the credit value. Conversely, if a large amount of content that interferes with a friend is sent, the user will automatically receive a certain penalty according to the user's report. The content sent by the user, no one will delete it, record the hash value through the blockchain, and the user enjoys the copyright no matter how many times it is transmitted.
Event marketing	Users can pre-store 1,000 USD to send announcements in the circle of friends and declare that all friends who support this announcement will automatically receive 1 USD reward after the event, and all friends who forward the message will automatically receive 10 USD reward. Until the 1000 USD is sent.
Numbers game	The user set up an entertainment group. After the game starts, the game currency is automatically redeemed. If you start a small online game, you will automatically team up after entering the game. The proceeds you get in the game, including gold coins and virtual items, can be seamlessly traded in the group.
Live video	If the merchant can set up, all the viewers who participate in the live video broadcast can automatically obtain the sharing link of the video and obtain the coupon of the organizer, and the coupon is

	automatically entered into the user's account. Anyone who watches this video lecture must pay a fee before joining.
Automatic car rental	If you use the QR code to take a photo, the deposit will be automatically deducted, and the vehicle will be unlocked automatically. This scenario is typical of offline applications because the underlying technology of automated car rental uses the blockchain's smart contract technology.

8 ECONOMIC MODEL

8.1 Ecosystem

Ecosystem of the
entire TokTok, including ordinary users, storage node, a
relay node, business customers, advertisers, developer’ s community, f
oundations, companies operating entity, an integral part
of several miners.

general user

Ordinary users download the client software, run light
purse (Lightweight Wallet), not all of
the books stored information, thereby reducing the storage burden on the user side, to reduce the cost of the loss of the network.

Relay miner

Theoretically, any node block chain, can be used as a relay node.

Storage miner

Storage node, a node can relay one, depending on the resources and the will of the participants.

Merchant customer

Companies can post blog for followers to subscribe. The platform uses smart contract technology to support flexible billing methods and fast billing mechanisms.

Advertisers

Advertisers can place ads on the platform. Only when the user authorizes,

the advertiser can analyze and push the advertisement according to the user's behavior data. Advertisers or BI companies need to pay users a certain amount of data usage fees.

Developer community

Developers include TokTok network platform developers, client developers, further comprising providing intelligent plug-ins, props, expression, or applet developers to TokTok network of developers as individuals involved, it can be the identity of the enterprise involved. TokTok allows the group owner to select a custom group template created by the developer, which runs on a third-party public chain.

8.2 Platform Value

Value of the entire platform, mainly reflected in the value of communication, storage and Media Values three major components. The value of communication, that is, the message sent by the user can be transmitted, and the user can communicate in the form of text, voice and video. The storage value, that is, the user's avatar and moments data, can be permanently stored, and no one other than the user can delete it. Media value, that is, when the entire platform of the future growth of active users, will form eyeball economy, advertisers and businesses have urgent needs, need

to publish some of the ads to this ecosystem, to attract the user's attention and form interaction.

8.3 Benefit-Driven Mechanism

Only by allowing all participants are profitable, then this ecosystem can really get up and running. If this product does not solve the user's pain point problem, the product experience cannot attract users and retain users, then the entire ecosystem has no basis to start and run. If the storage node and the message forwarding node are not motivated, the user's data cannot be stored, and the message sent by the user will not be quickly transmitted, and the user cannot communicate smoothly. If the foundation and operating entity companies cannot have basic working capital and a clear profit model as a guarantee, then the entire ecological operation lacks an organizer and planner. If merchants and advertisers are not able to benefit from media value on this platform, they will not be involved, and the cost of the entire platform will be shared among the foundation and users. If foundations and operating entities do not have sufficient funds to operate the platform and then all costs are shared to users, such platforms will be somewhat uncompetitive compared to traditional, free instant messaging platforms.

Therefore, under the premise of free use of the basic functions in protecting users, allowing cost-sharing by the entire ecosystem up and running, mainly merchants and advertisers, and that there is a very high demand both for the flow of the platform itself. Therefore, it is very important that the initial period of the platform requires certain financing to develop products and promote the accumulation of active

users throughout the platform. Then, the entire ecological cost bearer will be mainly merchants and advertisers. In
this ecosystem, there is provided a storage node and message forwarding service, will get excited, because they can profit on this platform, it will be actively involved.

Because the entire ecosystem participants to conclude them by means of a self-government of the organization, so the ecological token primarily to ensure clear responsibility and rights, rather than as the main users use means "micropayment" of. Therefore, this transaction speed and capacity of the tokens, not so demanding for consensus needs no prescription required, satisfactorily resolved through BOLT technology, which reduces costs.

8.4 Community Consensus

The consensus exists in the consensus of community management, the consensus of platform operation and the consensus of token incentives. Intentional community management, is that the whole community recognized core values decentralized "micro-letters", giving the user the freedom of speech, to get rid of any government regulation, the pursuit of safe, reliable storage of personal account data, maintaining ownership of the user's digital assets and The right to use , to maintain the ecological distribution of fair benefits .

Token incentives consensus exists in the operation of the infrastructure and operation of the entire ecological system. And traditional public consensus mechanism different chains, they have taken POW or POS as

a basis for consensus on the need to open the books and smart contract and verify the implementation of priority performer then get excited tokens. Consensus of this project is to provide storage resources and decentralized to send a message to the entire ecosystem, you can get excited platform. This incentive mechanism, the entire ecosystem needs to reach a consensus, if there is a fair question, it will restrict the ecological motivation to run, will affect the enthusiasm of the participants, the entire ecosystem is difficult operational. To this end, the consensus economic incentive token, it is vital, need to plan scientific and rational way.

For storage nodes, Proof-of-Replication (PoRep) and Proof-of-Spacetime (PoSt) are used as the consensus mechanism . The obtained token is determined based on the storage capacity and storage time of the contribution of the storage node. The token is released every 24 hours. Participating storage nodes, you need to run the client software provided by the Fund. All stored files are distributed and distributed in fragmented form, so if an individual node has an accident, it does not affect the integrity of the user data.

For relay nodes, using a consensus Proof of Relay mechanism. This scheme is charged based on the number of network bytes passed by the relay node. The higher the number of bytes, the higher the number of the billing token. The settlement period of the token is settled every 5 minutes. For storage nodes, each node stores redundant data fragments to ensure the integrity of the stored data, even if a single node fails , does not affect the user's data integrity . For relay

nodes , you need to ensure a stable and efficient operation of a single node . In addition to the normal nodes , for high-performance super nodes , as a backup solution .

After commissioning the product, when you run the whole ecosystem starts, the Foundation will host a super node election campaign. We encourage ordinary node is also involved, but the algorithm of the system is to impart better resources according to the operating speed of the server with more tokens incentives. For storage super nodes, you also need to assess the speed of storage I / O , and also encourage higher quality storage system intervention based on I / O speed as a parameter .

User contributions for media value, according to the Proof of Contribution for judgment. About Proof of Time and Space, Proof of Relay and Proof of detailed formula Contribution, it will send special report published. Platform operated by consensus, which includes an open and transparent management of the foundation, details will be discussed in the management part of the foundation of the subsequent releases.

8.5 The Utility of the Token

As mentioned in the above section, the main purpose of tokens is to establish a responsibility mechanism to promote the entire ecological operation, and not as a major micro-payment means for users to purchase virtual items such as props . Well, this token, how can assume

such a role, and together the various participants play from such an effect?

First, tokens are a cash equivalent that participates in the ecology and provides resources. The operation of the entire ecological, economic resources and energy needs (mainly electricity), will be divided into the smallest unit cost, is the essence of the tokens. Thus, by forwarding the message relay node or assume the power consumption (power may be hashed directly calculated), and providing storage for use by others, it earns tokens.

Tokens are used as evidence to contribute to the ecology, and the redemption is mainly for merchants, advertisers and ordinary users with value-added needs. The three parties honor must provide this token, we can use the resources of the platform. Thus, the ecological cost of consumption, and media value, the value of storage, communications value on the corresponding up.

In the platform, merchants need to push messages, and need to store additional public content, you need to consume tokens. Users need longer calls, extra permanent storage, and paying tokens. If you need to deliver advertisers advertising platform, but also need to pay token. And the only way to earn money to replace only be obtained by increasing the media value, value storage and communication value of the platform.

Pay the token:

- Serve ads (consume media ad slot resources)

- Purchase storage space (consuming storage resources)
- Purchase communication duration (consuming communication resources)
- Smart Group Chat template, use of space

Earn coins:

- Provide storage space (improve storage value)
- Provide message forwarding service (improve communication value)
- Provide high quality content and get praise from users (improve media value)

8.6 Anti-attack and Early Incentives

For early ecological operations, resources are extremely valuable, because the storage and communication supply nodes do not form a trust in the future development of the platform, so the foundation and operating entities need to pay the fees to adopt. This time, the user plenty of storage and communication, will constitute a very high cost. To do this, you need to set storage and communication resource consumption thresholds. When the number of active users on the platform increases, media value, storage value and communication value (hereinafter referred to as the three major values) can attract merchants and advertisers to participate in the cost sharing , then the threshold of storage and communication resource consumption is gradually relaxed , giving users a kind of participation. the more, the cheaper the sense of. At the same time, due to the

increase in the number of participants, the unit participation cost of the entire ecology will be reduced due to the scale effect.

Early incentives, reflected in how to pull and attract users, and how to attract storage and pull the relay node play ecological values. For the user, the dialogue is mining, the call is mining, the "moments" is mining, the article is mine mining, the friend is invited to mine, and the matching address book is mining mode . For storage and relay nodes, early mining gains were high, achieving a halving mechanism every four years. The whole foundation should be set aside certain funds to promote the tokens can be exchanged for coins become legal tender or bit, and then gradually build confidence in the market, so that the entire ecological stability thrives and develop. The total supply of tokens is constant, and the total circulation should not be too large, giving participants a value-added expectation. At the same time, to create a harmonious ecological culture, are very beneficial to the entire ecosystem of start.

8.7 Token Issuing Plan

The total amount issued for the entire ecosystem tokens 21, 000, 000. Of which 40% as a pre-mined token, of which 15% of the original motivation for the team, 15% for private equity and 5% for the Foundation set aside 5% incentive for early ecology. The remaining 60% of the parts, can only be generated by a node by providing communications and storage resources. By these tokens generated by mining, the implementation mechanism of halving every four years.

The Foundation reserves 5% of the tokens. Used to ensure the long-term development of the Foundation. These tokens are initially not in circulation, after locking three years, the release of 1% per year. The team holds 15% of the tokens, implements the lockup mechanism, and releases 4% of them after the listing. After that, 2% of them are released each month, and the release is completed in four years. Investors involved in 15% of the tokens listed the release of 10%, then15% per quarter release, release year and a half to ecology.

For 5% of the tokens ecosystem incentives, which is the main mining through dialogue, a call that is mining, made popular articles namely mining, invite friends namely mining, mining of pattern matching address book that is paid to the ecological system.

9 CONCLUSION

Traditional mobile instant tools have many implied problems that are going to be properly resolved by TokTok 's distributed storage, communication and encryption technologies. The rise of the Value Internet will give birth to abundant application form, these applications will be present in a variety of scenarios online and offline. This trend is irreversible. We are convinced that DApps will eventually spread, block chain technology will affect every aspect of people's lives. When this day becomes reality, it will be expected that TokTok App will replace WeChat to become a more powerful digital life essential tool.

In the book " Blockchain +" written by Du Jun who founded Node Capital, Mr. Du vividly explained the use of the blockchain 3.0: "When a baby born, the doctor uploads the child's birth date and other information. To the blockchain citizen electronic identity system, after the system confirms the child's information, the child will be assigned an ID. After the ID is confirmed by the relevant government department, the relevant electronic identity information will accompany the child's life. After that, the child's student status, health, Information such as property, title, credit, etc. will be linked to the ID and stored in the blockchain. When it dies, his wills will be triggered, his property will be distributed to his heirs, and information about him on the system. The chain will no longer add information."

For the Enthusiasts and pioneers of blockchain technology, the judgment that future blockchains affect all aspects of people's online life will become a reality. As people build networks and IM identity, the

main tool of life participate in the network, will play an important role in people's digital lives. We build the TokTok App, not only to solve the security and privacy protection issues of traditional IM , but more importantly, she will develop into a next-generation instant messaging network platform , which will eventually become a hub for people to participate in the digital economy and exchange value. .

FAQ

1. One of the core design ideas of this system is that, according to the definition of " TokTok " , information is transmitted on the blockchain ,or at least decentralized, and should not be subject to a corporate entity. Controlled centralized systems to handle information dissemination. In this case, how should our system architecture handle massive amounts of one-to-many (such as group messages, 1 to 100) message propagation, especially how to achieve high performance (mainly low latency) , and high efficiency (not Let the processor and bandwidth do nothing ?)

In the network system of TokTok , there are network elements such as relay nodes . The relay node will serve as a bridge messaging, contribution to the ecological communications messaging value. For performance and efficient handling mechanism, taken Proof of Relay consensus mechanism, i.e., throughput and network messaging will directly affect the execution rate of return node, it is possible to push the entire network relay node competition, prompting transmission speed and throughput continues to increase. For a one-to-many group message, if a message sent by one user is transmitted to each group user separately, serious resource consumption is caused. More flexible handling mechanism, the group itself as a form of users, each user in the group to speak in, the equivalent of a message to a user group, and user group information received , and then distributed to the group in Every user except the user . Therefore, if it is a 100 'group, wherein any one message, the message sent by the user 1 times, then the user is transmitted from the group 99 times , a total transmitted 100 times . If a user group

send @ messages, the situation is somewhat special, but also needs to be sent to the @ reminds the user's information.

2. The client of TokTok is the same as the client of WeChat itself. It is possible to have multiple instances at a certain time (for example, the desktop and mobile phones are online at the same time). Can the above architecture effectively handle such a situation?

For the case where the user logs in at the same time of multiple terminals, the system adopts a multi-terminal message synchronization mechanism to ensure that each terminal can receive the same information. When multiple terminals log in, the system will monitor the IP and port number of multiple users logging in. When a message is transmitted, it can determine which terminal the user is currently inputting, and then synchronize the message to other users. A terminal that is not actually operating.

3. The client may be offline for a certain period of time. Can the information received by the user be lost during this time? How can our architecture do this if it can't be lost in whole or in part?

For the case where the client is not online, the information received by the user is temporarily saved in the IPFS cache. When the user logs in, the part of the information is automatically forwarded to the recipient. The system will set the capacity for sending messages. For large-capacity messaging, such as with file transfer, the software will automatically prompt how long the file will be saved on the server. If it is over a certain period of time, it will be deleted. If the user needs the file to be stored on the server for a longer period of time, the user has to pay a certain fee.

4. Since the system for processing information needs to be decentralized (see first article) , then when the case of partial node temporarily or permanently offline , the system in the overall level of how to ensure continued reliable operation , correctly handle the information for all users ?

If the storage node temporarily stops working or goes offline, there is no impact on the data stored by the user in the decentralized cloud. Because each storage node only stores partially fragmented information, the storage system of the entire system is redundant. For the relay node where downline by the super relay node as a backup link, will automatically and quickly switch to another relay node. The system uses a distributed hash table to store the IP address, port and online status information of the logged-in user. When a node is temporarily offline, it does not affect the normal operation of the entire network.

5. Dealing with customer information These system nodes should rely on what incentives to keep them online and try to process as much customer information as efficiently and quickly as possible.
As in Chapter 6.3 of this white paper, for relay nodes and storage nodes, according to the consensus mechanism will be corresponding incentives.

6. What is the incentive mechanism for the ultimate user, how to design it to be simple and effective, and attractive to users, but also to promote active user growth?
We will use the dialogue that is mining, mining namely calls, issued a "circle of friends" that mining, made popular articles namely mining,

invited good friend or mining, mining of pattern matching address book that is to attract active users grow.

REFERENCES

[1] Protocol Labs. Filecoin: A Decentralized Storage Network. July 19, 2017. URL https://filecoin.io/filecoin.pdf

[2] Storj Labs, Inc. Storj: A Decentralized Cloud Storage Network Framework. October 30, 2018. URL https://storj.io/storj.pdf

[3] Vinnie Moscaritolo, Gary Belvin and Phil Zimmermann. Silent Circle Instant Messaging Protocol. December 5, 2012. URL https://netzpolitik.org/wp-upload/SCIMP-paper.pdf

[4] Sebastian R. Verschoor, Tanja Lange. (In-)Secure messaging with the Silent Circle instant messaging protocol. 2016. URL https://eprint.iacr.org/2016/703.pdf

[5] Moxie Marlinspike. The Double Ratchet Algorithm. 2016. URL https://signal.org/docs/specifications/doubleratchet/doubleratchet.pdf

[6] MOXIE MARLINSPIKE. THE X3DH KEY AGREEMENT PROTOCOL. 2016. URL https://signal.org/docs/specifications/x3dh/x3dh.pdf

[7] Forrest Pieper, Will Drevo, Colin Taylor. Peerchat: a Distributed, P2P Communication Network based on Kademlia. May 4th, 2014. URL http://css.csail.mit.edu/6.824/2014/projects/drevo. Pdf

[8] Maymounkov, Petar and David Mazieres "Kademlia: A Peer-to-peer Information System Based on the XOR Metric" Peer-to-Peer Systems. Springer Berlin Heidelberg, 2002. 53-65

[9] Goldoor, Abe" Update on BitTorrent Chat." The BitTorrent Engineering Blog., 19 Dec 2013.

[10] Bryan Ford, Pyda Srisuresh , Dan Kegel. Peer-to-Peer Communication Across Network Address Translators. URL https://pdos.csail.mit.edu/papers/ P2P nat.pdf

[11] Jeffrey L. Eppinger. TCP Connections for P2P Apps: A Software Approach to Solving the NAT Problem January 2005.