Blockchain-Based Distributed Protocol
OpenChat White Paper

OpenChat Project Team
Version 3.0
2018/03/01

Content

1. Background Introduction

1.1 Blockchain Technology

Blockchain is one of the most revolutionary and disruptive technologies of all time. Above all, blockchain represents a new social direction of thought, which indicates the arrival of a new era of human transition and change. Kevin Kelly describes in "Out of Control": “The laws of evolution of nature, society, and technology will shift from a biological logic move from edge to center to edge, from uncontrolledness to control to uncontrolledness”. The technical basis of the blockchain is the distributed network architecture. It is precisely because of the maturity of the distributed network technology, which evolved from systems orbiting the center, to weak center, sub-center and then to shared, consensual, decentralized organizational structure, that commercial architecture can be effectively established.

There have been several iterations of blockchain technology today:

1. The first is a distributed ledger. It is a general ledger for all agencies and a general ledger for all business matters;

2. Second, blockchain technology is a new type of database. There is no central computer room, there is no operation and maintenance personnel. The third party enters the data according to the consensus algorithm, the use of asymmetric encryption algorithm ensures data security;

3. Third it is a smart contract. Relying on smart contracts, the world is like a supercomputer running fine, everything can be agreed in advance. Compiled into code, in accordance with the procedures;

4. Fourth, it is a TCP-IP model Point-to-Point value transfer protocol. Its invention marks the fact that internet technology has helped people to transmit information more efficiently over the past two decades. You can start helping people to realize value interconnection without the help of third-party trust endorsement.

The core value of blockchain lies in its realization of a tamper-proof, secure and reliable distributed accounting system. Multiple participants using blockchain ledgers can form the basis of trust for multi-party transactions without the need for additional third-party to guarantee the transaction, thus enabling a low-cost, low-latency information exchange and processing system to enable the efficient flow of digital value.

1.2 Digital Currency Encryption

Encrypting digital currency is an important application on the blockchain. As the name implies, cryptocurrency concentrates on cryptography. Cryptography provides a mechanism to encode cryptocurrency rules into the system itself. Not only can people use cryptography to prevent interference with the system to avoid confusion, it is also used to code currency units into the mathematical protocol.

The concept of encrypted digital currency distributed by social networks based on the BIMP distributed protocol implements this concept. Relying on the unchangeable, safe and reliable attributes of the blockchain creates a peer-to-peer

community allowing everyone to conduct encrypted digital currency transactions and exchanges.

1.3 Instant Messaging Software

With the popularization of smart phones, instant messengers gradually replaced traditional 2G SMS and voice calls in people's daily life. In countries where mobile communications are developed, instant messaging software (IM) such as WhatsApp, Telegram, WeChat has greatly facilitated daily life and communication. The majority of the population in emerging countries, especially urban residents, are in high demand for "IM + e-Payment" models. Instant messaging software and applications has become a platform to build advertising, mobile games, e-commerce, peripheral services and other value-added services. Constructing a well-established online ecosystem in emerging markets and creating a “one-stop shop” for emerging market individuals and businesses is where the OpenChat team is fully committed.

While IM software is developing rapidly, traditional enterprises has gradually exposed some of the problems in their operations.

Traditional IM applications usually include three parties: platform, partners and users. Each side has a role to sustain the development of the platform. Although everyone plays a key role, the goals of these groups are very different from on another. The current model does not provide a means by which their incentives can coexist and harmonize. Driven by the supply side's own interests, the future of social networks becomes problematic. The platform and partner associations do everything possible to gain access to users' information in order to extract big data

to analyze as a basis for promotion. However, this has caused a serious privacy crisis.

In 2013, Facebook, Skype, Microsoft, Apple and Yahoo! were exposed to the Prisoners Project being implemented by the U.S. National Security Agency, causing an uproar. As a user, you may have done nothing wrong, but you may become the subject of suspicion and surveillance. The project had the potential to scrutinize all your past decisions and review all the friends you've talked to, and you might be penalized for just sending the wrong message once. Nowadays, users in some countries pay more attention to personal privacy, but people in other countries may not care what their authority is doing and also may not care about the privacy policy statement in software apps.

In 2016, a "Social Software Communication Privacy Ranking" released by Amnesty International was widely distributed on social networks. This list compares and rates current mainstream social software services from five aspects: "Human Rights Protection", "End-to-End Encryption", "Risk Alert", "Open Door to Open Door" and "Publishing Encryption Technology Details". As global mainstream IMs Skype and WeChat scores were only 40 points and 0 points (out of 100 points). The ranking shows the seriousness of the risk of privacy disclosure. The traditional method of information encryption technology is called "transmission encryption." Service providers use different encryption methods to encrypt the transmission of information. The biggest drawback of this encryption method is that the messages sent between users are plaintext. In other words, if the service provider in charge of information transmission wants to peek at the privacy of users or inadvertently

release the information, all the user's chat records are unreservedly exposed to the public.

The prospect of a troubling future is no longer the disclosure of personal information, but the prediction of user behavior. When the development of technology advances to a state where artificial intelligence (AI) can predict, affect and direct people's decision-making. When the intellectual property and algorithms of these AI are controlled by a large corporation, the ethics of the application of the technology comes into question.

Blockchain is a new composite application mode of computer technology that includes distributed data storage, point-to-point transmission, consensus mechanism and encryption algorithm. Blockchain, as a strong guarantee of digital assets, has been well received by the industry. However, the traditional IMs, which should be responsible for the privacy of users, does not provide any corresponding entry point to the blockchain. At the same time, providers of traditional IM third-party products are constantly competing with each other to ensure their own interests. They simply can not enter into a state of mutualism and mutual benefit. Over time, as products become more homogeneous, the industry will gravitate towards acquisitions and mergers, with some products being eliminated from the market. This not only harms the diversity of the market but also stifles many great ideas.

1.4 Electronic Payments

Electronic payment methods can be classified based on two basic concepts of cash and credit.

Credit card transactions are currently one of the major online payment methods. For example, a user is shopping on Amazon. First you need to enter your credit card information when billing. Amazon receives the account information and feeds back to the payment "system" the information processor, bank, issuing company and other intermediaries.

If using a third-party payment facility such as PayPal or Alipay, the user experience model would be for the intermediary company to collect the user's bank card information and approve each transaction information and settle the payment with the seller at the end of each trading day.

Credit-based electronic payment is convenient, but its security cannot be guaranteed. If either the buyer's user information or the payment channel itself are compromised, then the payment system will be susceptible to harm. The cash-based payment system, however, increases the payment system complexity while avoiding the security risk of providing bank card information directly to the buyer. Users and sellers can not communicate directly. They have to open an account with a third-party payment company.

Encrypted digital currency, represented by bitcoin, supports both user-merchant transactions and transactions between users and users. In fact, the Bitcoin system does not distinguish between users and merchants. Much of Bitcoin's success is due to its support for transactions between users and users. From the beginning, every bitcoin user can send to other bitcoin users. As a result, cryptocurrency is likely to become a substitute for credit card companies and third-party payment

agencies in the future. It will truly deliver point-to-point real-time trustless transactions as the primary choice for electronic payments.

In addition, whether it is based on cash or credit payment, cross-border payment with high fees are one of the pain points of the market. According to the McKinsey report "2016 Global Payments: Strong Cornerstones Despite Changes", cross-border payment transactions account for less than 20% of global payments. However, the transaction fee it brings is 40% of the worldwide payment transaction fee. In 2015, the cross-border payment revenue was 300 billion U.S. dollars. Improving efficiency and reducing costs for is an urgent need that blockchain technology must address.

2. OpenChat Ecosystem

The OpenChat project is a set of distributed protocol BIMP based on blockchain technology. The first floor-to-ceiling application of the BIMP protocol will be:

1. Instant messaging platform with an add-on light wallet application based on the blockchain cross-link technology (partially implemented);

2. Social networking platforms using decentralized technology which will build a completely new social-networking ecosystem in the future (partially implemented);

3. Exchanges that use the protocol and tokens as a voting mechanism (currently in discussion with several leading exchanges).

OpenChat team is actively discussing with these strategic application partners to implement the protocol and circulate the token. ChatCoin tokens made by the BIMP protocol are widely supported in BIMP-based chat tools. It is used on the platforms to issue, reward, pay users and will have a wide-ranging of practical applications.

2.1 Instant Messaging Project (IMP) Introduction

The instant messaging platform built on the OpenChat protocol is a platform to consolidate and support multiple blockchains using the "IM + wallet" model. The model uses instant messaging software as a platform to build advertising, mobile games, e-commerce, peripheral services and other value-added services,

eventually becoming a stable sustaining online ecosystem. For users, it is a “one-stop shop” platform to handle all personal and business matters.

IM is the foundation for the project development. As many assets in emerging countries and markets have not been digitized, such as housing, automobiles and so on. But in the future, when more assets are digitized or moved onto the blockchain, IMs can realize the agreement with ChatCoin to inspire the community's development capabilities for better circulation of these digital assets. This in turn drives ChatCoin's acceptance and circulation.

The complexity of the technology facing the first generation of cryptocurrencies is often too intricate for most consumers. Transaction costs, private keys, and alphanumeric address issues create barriers for mainstream users. These include the common requirement to hold cryptocurrencies first (only cryptocurrencies must be held before the other tokens can be acquired and utilized). OpenChat will try to greatly reduce this type of friction and grant users a user-friendly entry point to the blockchain. Prior to being able to interact with ChatCoin, user-initiated processes do not require them to hold cryptocurrencies.

The IMP maintains the Community of Interest Principles, which protects the interests of users and developers and unites everyone involved in improving and promoting the project. But the decentralization of the IMP does not mean it is an anarchist disposition, but rather a platform that can help societies resolve the issue of trust in social activities at low cost. It is an effective means of promoting the establishment of an honest and trustworthy (or trustless) society.

2.2 Blockchain-based Electronic Wallet

The main function required to enable the digital community to use cryptocurrencies is a wallet. As a first step, the IMP will consolidate the wallet for each user account. The associated user interface will allow the most common wallet interaction and support millions of active users by consolidating their wallets. The wallets have the potential to become the most popular and used cryptocurrencies wallet in the world.

2.3 Self-media (Personal Media) Ecosystem

This tool is a dynamic display of all your social activity, news, quotes, transactions in one platform. Information about the activity of friends can be found alongside the activity of their own blockchain transactions.

This feature is actually an effort to nurture users' habits of rationalizing blockchain wealth. Because of the focus many users place on messaging and social networking, there is no sound financial literacy for digital assets. By displaying social activity and blockchain metrics together, users can look at the what their friends are doing but also be aware of their own digital asset-related changes in the market. This will help users develop the rational use of digital assets and configuration habits.

2.4 Social/Chat Function

With the chat function, users can keep contact with family and friends and establish their own social circle. Users can also share other decentralized apps on the platform with their social network. The platform offers the fastest mobile communication with HD video, voice and text. It uses a unique distributed

technology, highly secure encryption service to ensure fast and free communication. The platform boasts delay-free, high-quality voice/video calls and supports over 30,000 users for simultaneous group chats.

As the product user base grows in size, each user's social structure will further merge with the instant messaging platform over time. The social relations such as family, friends, acquaintances will extend to work/professional connections, and ultimately all connections to form a global social system.

2.5 Application Network (Network)

The Application Network is a global, decentralized, symbiotic application market that OpenChat offers. Users can download the products provided by third-party application developers here. The user gains access to the app by paying or providing valuable action/activity. Developers earn ChatCoin by issuing DApps.

OpenChat will maintain and monitor the network, making timely adjustments to the developer reward strategy to maintain the stability of the symbiotic environment. At the same time, OpenChat will encourage more developers to provide innovative DApps.

2.6 Qtum-based System

The platform needs a medium for operations before users can interact and trade with each other. Traditionally, this medium was provided by a reputable network owner. However, with the advent of the common foundation of quantum chains, we can provide users with a decentralized, de-licensed, trustless, and cryptographically verifiable protocol that grants fair access.

As the quantum chain evolves, the world has the technology necessary to create a better model of the Internet. We think the Qtum team will continue to disrupt financial technologies, the Internet of Things and decentralized applications.

Qtum will eventually become a social technology. In order to realize its perceived potential, we need to maximize the utility of non-technical users. It needs to be ubiquitous, always accessible and needs to be part of our everyday life.

3. Economic Model

OpenChat is committed to creating an open source symbiotic economy. Under this system, all participants (users, DApp developers) will become a community with shared interests. The community must all work together to win common interests. With the continuous increase of participants, this system will also expand indefinitely.

As a user, ChatCoin rewards provided by a DApp developer are granted by proof of valuable activity (clicking on an ad, sending a link, etc.). This not only enhances the user's active ability but also reduces the developer's promotion cost, realizing the common promotion of benefits.

As a DApp developer, in this open source symbiotic economy, they can learn from each other and share each other's technological expertise and finding out their own shortcomings. All developers can really connect into a community of interests. Everyone will work hard to develop better applications. OpenChat, on the other hand, offers lots of ChatCoin rewards to developers who make significant contributions to technological advancement to motivate more developers.

4. Business Model

4.1 The New Digital Lifestyle Service Platform

OpenChat partners will launch several market use cases that will allow consumers and brands to use ChatCoin. Through experimentation, OpenChat partners plans to iterate through products for users to create unique two-sided market applications. On the supply side, automated programs or content creators will create unique experiences. On the demand side, users will consume such products or services. OpenChat partners' automated programs will be able to form their own unique business model in the near future.

4.2 Application Scenarios

In addition to social scenarios, point-to-point wallets allows users to fully inter-operate in transactions. E.g.:

▸ *Scenario 1:* User A is an Egyptian user. However, he has to live and work outside his home country in United Arab Emirates. In his spare time will use OpenChat protocol IMP to make transnational calls with his family. After receiving his salary, he can send money to his family through ChatCoin. This eliminates the need for expensive currency exchange and transfer fees.

▸ *Scenario 2:* User B is a music enthusiast who loves newly released music. He can buy online music directly with the OpenChat protocol wallet.

▸ *Scenario 3:* User C is a Chinese user who intends to bring his family to travel abroad on holidays. Before going abroad need to exchange a large number of

foreign currency. Each bank before and during the trip will draw a transaction fee. On the way to travel, the traveling family will always have to worry about whether the money they are carrying is safe. At the end of play, you also need to convert the leftover foreign currency into the home currency. The process is very complicated. If the OpenChat protocol wallet is used, currency can be paid directly when it is spent online or offline, and the excessive fees at every point during the trip can be avoided.

▸ *Scenario 4:* User C intends to invest in vacation real estate but finds that the price of a domestic house is already at a high price. Some overseas countries are attracting more and more people to travel there on holiday. This is a great opportunity to buy a vacation home overseas. So user C uses the OpenChat protocol wallet to buy a house in the Bahamas without excessive cross-border transaction fees.

5. Project Implementation

OpenChat protocol applications and OpenChat protocol partners have debuted on the Apple App Store (App Store) and Google Play. Users can download and use OpenChat-based software directly or visit the official websites.

6. Governance Mechanism And Risk Management

6.1 OpenChat Investor Community

OpenChat will build a decentralized international community and set up the OpenChat Foundation to ensure the management and operation of the OpenChat investor community and fund security. The OpenChat Foundation's organization will consist of the OpenChat Investor Community Conference and the OpenChat Foundation Autonomous Council and Executive Committee.

- The OpenChat Investor Community Conference is the supreme authority of the OpenChat project. It consists of all ChatCoin holders. All holders are able to exercise their voting rights through Community Meetings and participate in decision making on major issues of the OpenChat project.

- The OpenChat Foundation Autonomous Commission is responsible for Investor Community Meetings. It is responsible for the executive management and oversight functions of the Executive Committee. The Autonomous Commission will annually make adjustments to suit the changing market environment, such as the number and currency of tokens held.

- The Executive Committee is responsible for the community councils and investor communities. It consists of OpenChat project's technology development and day-to-day operations team. It is mainly responsible for OpenChat project technology development, ecosystem construction,

operation and maintenance services, community management, and other functions.

- OpenChat Investor Community Meeting

  The OpenChat Investor Community Conference, comprised of all ChatCoin holders, is the supreme authority of the project.

  The OpenChat Investor Community conference has the following functions:

  (1) Modify investor community conference management regulations;

  (2) Supervise the implementation of the management regulations of investor community meetings;

  (3) Election and change of members of the self-government committee;

  (4) Undo undue decision of the self-government committee;

  (5) Approval of major business issues and changes

  Members of the community will make resolutions through the form of voting to be held by the holders based on the number of coins held in ChatCoin and the weight calculated by the vote tally. The community meeting is held annually. The General Assembly will conduct a report on the work progress of this year's project. If the Autonomous Commission considers it necessary for more than one-fifth of the ChatCoin Holder's approval to hold a community meeting.

6.2 Risk Management

ChatCoin, through the blockchain consensus, decreases the risk of tampering with decentralized technology and digital signatures, end-user encryption wallet and other security measures to ensure that user accounts are secure. User transfers, red envelopes, built-in trading platforms, etc. will provide financial-grade security services through Qtum to integrate data and transactions into the blockchain, building a secure trading environment.

6.2.1 OpenChat Audit

Foundation strictly abides by the relevant laws and regulations and industry self-regulation, providing completely transparent financial management. Each year, the OpenChat Foundation invites internationally renowned third-party auditors to audit and evaluate the use of funds, cost and profit distribution of the Foundation. The Foundation will make an unqualified public third party assessment and audit result.

6.2.2 Information Disclosure

The OpenChat Foundation will regularly disclose project development progress, news and capital usage. The OpenChat Investor Community Meeting will vote annually on the audit reports issued by third party auditors and the annual progress of projects announced by the Executive Board. The Executive Committee will also make immediate progress reports on the project according to the actual development of the project, through announcements, official website and various social networking platforms.

7. Project Development Planning

7.1 Future Outlook

As internet technology reaches maturity, human society has created more applications in the digital space that is exclusively available for the digital realm. The traditional mode of relying on land, equipment and labor to create wealth is constrained by these limited resources. The infinite scalability of digital space, the infinite reproducibility of bit structure, and the multidimensional plasticity of the virtual world may mean that wealth can be created digitally, with its scale and its multiplier effects being tens of times more than that of the physical world. These new forms of wealth are digital assets. However, driven by huge profits, many enterprises are more inclined to compromise the rights and interests of users in return for their own rapid development, the most widely breaches are undoubtedly the user's personal information and privacy.

OpenChat is a fast growing, open source community. We hope to establish a strong digital life platform, serving every OpenChat protocol application user's digital life. OpenChat will later build a new decentralized social economy network. With highly protected users, an automated user-motivated engine and a multi-linked billing system will allow hundreds of millions of users to truly enter the new digital economy.

In the future, OpenChat users simply need to pick up the phone to easily discover the best ways to make money through utilizing the artificial intelligence in the platform. Wealth can be created by just moving your fingers. If the user also want to create value but also want to accept the task of creating wealth for other users,

they can do so and their reward in ChatCoin will be commensurate with the amount of productivity they have created. Everyday, the wealth and token productivity will be ranked on a list to display who amongst your connections has created the most value.

OpenChat is committed to bringing the digital economy into everyday life. We will do our utmost to promote the era of decentralized social economy network. With its huge subscriber base, OpenChat protocol applications are set to become the maker of the next generation of IM rules and dominate the future of a digital economy.

If you want to be a navigator of digital life in the future, you must know the key to the future. OpenChat is confident that this key will be handed over to you and will lead you to the pinnacle of your future life.

8. Team Introduction

8.1 Team Background

The support team behind OpenChat is an open source organization founded by members of the former Google technology team. It is committed to cross-border instant messaging application development and technological innovation. The company brings together members from Google, Huawei and other elite technology companies. The OpenChat team has developed a number of different useful applications delivered to different countries around the world. The products created by the OpenChat team have become an essential tool for daily communication for hundreds of millions of users.

At present, the instant messaging software independently developed and operated by the team occupies a competitive advantage in emerging countries. The company is committed to long-term, in-depth promotion of internet usage in emerging markets for network communications and personal communication, and to serve the majority of global users. The team will continue to consolidate and develop its existing market advantage in emerging countries in the future, with the core mission of building an instant messaging software as a platform to serve advertising, mobile games, e-commerce, personal services and peripheral services, constructing a well-established online market ecosystem, creating a “one-stop shop” emerging market life and work platform. In the Middle East, South Asia, Central and South America, Africa and other rapidly growing emerging markets, the team continue to promote these services and provide high-definition, safe, reliable, fast communication services and convenient mobile networking life experience. This will be the core mission of the global strategic plan.

8.2 Team Members

	Oscar
	Oscar is a senior Scrum expert and senior software engineer with many years of experience in team development and project management. His goal is to develop a top-of-the-line, globally-recognized software product.
	Nell
	Java engineer and commercial software consultant specializing in back-end development and micro-services architecture. Nell is a senior development engineer for our blockchain solutions.
	George
	Back-end and database senior software development engineer, good at software architecture and object-oriented design. Over the years, George has focused on the design of product solutions.

	Mia
	Mia has over 10 years of legal background, her expertise range from for profit and non-profit entity registration to start-up financing to solving legal challenges for start-up companies and SMEs. Mia has worked in the crowdsourcing and blockchain sector for many years.

	PikaOne
	UI/UX designer who has designed for many mobile products widely used today, PikaOne has many years of design experience at Google, and has a deep background in innovative design research.
	AC
	Brand interaction and concept designer, with years of experience in graphic and advertising design, he is now working on digital design and development.

References

[1] A. Narayanan. J. Bonneau. E. Felten. A. Miller. S. Goldfeder. *Bitcoin and Cryptocurrency Technology: A Comprehensive Introduction*. The China Citic Press, 2016. [2] P. Wayner. *Digital Cash: Commerce on the Net (2nd ed)*. Waltham, MA: Morgan Kaufmann, 1997.