Coinone

Decentralized futures trading platform

Copyright Notice

This white paper is prepared under the leadership of the Coinone team. Plagiarism is strictly prohibited. If you need to reprint it, please indicate the source. At the same time, the intellectual property rights of all product design concepts, technical design schemes and technical solutions involved in this white paper belong to the Coinone team, and the core technical schemes have been applied for international intellectual property protection. For any infringement of intellectual property rights, the team will protect their rights and interests through legal means.

Coinone Team

Contents

1 Project background

1.1 Development stage of blockchain

Blockchain phase 1.0 - digital assets:

In early 2009, bitcoin network was officially launched. As a virtual currency system, the total amount of bitcoin is limited by the network consensus protocol. No individual or institution can modify the supply and transaction records at will. After the successful operation of bitcoin network for many years, some financial payment institutions began to realize that the underlying technology supporting the operation of bitcoin - blockchain is actually an extremely ingenious distributed shared ledger and point-to-point value transmission technology, and its potential impact on financial payment and even all walks of life may be no less than the invention of double entry bookkeeping.

Chained data block structure based on blocks: each node of the blockchain system selects a block node with packaging transaction authority through a certain consensus mechanism. The node needs to package the hash value, current timestamp, effective transactions

occurred within a period of time and its Merkel tree root value of the previous block of the new block into a block and broadcast it to the whole network. Since each block is linked with the previous block by means of cryptographic proof, when the blockchain reaches a certain length, in order to modify the transaction content in a historical block, the transaction records and cryptographic proof of all blocks before the block must be reconstructed to effectively realize tamper proof.

Blockchain phase 2.0 - Smart contract:

Around 2014, the industry began to recognize the important value of blockchain technology and used it in fields other than digital assets, such as distributed identity authentication, distributed domain name system, distributed autonomous organizations, etc. These applications are called distributed applications (DAPP). Building dapps from scratch with blockchain technology architecture is very difficult, but different dapps share many of the same components. Blockchain 2.0 attempts to create a common technology platform and provide CoinoneS services to developers, which greatly improves the transaction speed, greatly reduces resource consumption, and supports a variety of consensus algorithms such as pow, POS and dpos, making the development of DAPP easier.

With the deepening of blockchain technology and application, blockchain 2.0 represented by smart contract and DAPP will not only support the architecture of various typical industry applications. Behind the operation of various forms such as organization, and society, we may see the shadow of this distributed cooperation mode of blockchain. It can be said that blockchain will widely and profoundly change people's way of life. Blockchain technology may be applied to the scale coordination of human activities, and some even boldly predict that human society may enter the era of blockchain, that is, blockchain 3.0.

Blockchain phase 3.0 - underlying basic application of blockchain:

Coinone is a blockchain based integrated, social, open-source and integrated infrastructure of blockchain technology. The open source software designed and released is a branch application of bitcoin in the blockchain network. It is an information storage system based on blockchain, with digital assets in the form of P2P as the specific form. Unlike most currencies, Coinone does not rely on specific monetary institutions to issue tokens. It issues tokens based on the company's funds and the income from bitcoin computing power data. The computing power is gathered together to recharge Coinone tokens through collective mining. When the platform already has sufficient tokens, it will open the platform so that investors can trade on the

platform and exchange profits by trading. Coinone uses the distributed database composed of many nodes in the whole P2P network to confirm and record all transaction behaviors, and uses the design of cryptography to ensure the security of all links of money circulation.

1.2 Overall economic scale of blockchain

Blockchain has taken the lead in the exploration of the financial industry, and the application of other industries is also expanding rapidly. This blockchain technology revolution is sweeping all walks of life, such as finance, Internet of things, health care, intellectual property rights, public charity, education, supply chain, public security, energy and so on. From the perspective of regional market, the North American blockchain market accounted for the highest share in 2016. From 2016 to 2021, the compound annual growth rate in the Asia Pacific region will be maximized, and China will give priority to benefiting from the many potentials of blockchain technology.

According to the data of business research company, the global blockchain market is expected to reach US $15.88 billion in 2023. Although it fell 7.27% to US $2.27 billion in 20210 due to the epidemic,

the potential annual growth rate by 2023 is still more than 91%.

Tomohiro Maruyama, senior manager of PWC consulting, said that after the epidemic, more companies should adopt blockchain. The widespread digital transformation triggered by New Coronavirus will encourage people to use block chains to guard against fraud.

As for the future development of blockchain, there is an optimistic prediction that 10% of the global GDP will be stored by blockchain technology by 2025. The application value of blockchain has been widely concerned all over the world. Countries began to think about the development path of blockchain from the national level. China has synchronized with the world and launched relevant research and practice. Chinese concept projects will play an important role in this change. According to the survey of Coinone team, many heavyweight project investments in Silicon Valley come from the Chinese market. China has a large population and abundant traditional funds. The power of the market determines the flow direction of the project. 2022 is destined to be a crucial year for the development of DEX blockchain project.

1.3 Development trend of blockchain

Since 2018, the global blockchain seems to have entered a white hot development environment. Countries continue to introduce or update relevant regulatory policies, and the Institute of ICT released the development trend of global blockchain.

● **Trend 1: blockchain application scenarios are becoming more and more complex, and cross chain interconnection is becoming more and more important**

With the increasingly complex application scenarios, especially the integration with the real world, and the increasingly strong link collaborative operation, cross chain and side chain technology has become the key to realize the transmission of value network and the bridge for the outward expansion and connection of blockchain. The shift from physical assets to digital assets, online and offline interaction, chain up and chain down interaction, delay problems, parent chain bifurcation, and how to design the network structure are all issues that need to be paid attention to.

● **Trend 2: blockchain privacy protection mechanisms are diversified and become a key lubricant for activating commercial**

applications

Including ring signature, multi signature, mixer, zero knowledge proof, homomorphic encryption and so on. Looking for privacy protection algorithms suitable for the business field, especially combined with the real economy, is a road that must be taken.

● **Trend 3: blockchain security issues have attracted attention, which urgently needs attention and solutions**

How to build a blockchain security system around physical and data application systems is a very important issue.

● **Trend 4: blockchain causes policy supervision problems, and the two complement each other**

Using blockchain to supervise blockchain, especially the supervision technology in the financial field, can actually be classified as the problem of using technology to govern technology.

1.4 Development of blockchain digital currency

With the development of computer technology, mankind has

gradually opened the door of the digital era. PC and all kinds of software have made great progress and popularization in this era. For finance, it began to enter the stage of electronization and digitization. With the emergence of Internet technology and distributed technology, mankind has rapidly entered the information age. Big data, cloud computing, various software services and mobile applications have fully entered the lives of ordinary people. Financial services are also gradually developing and evolving in the direction of Internet, mobile and even intelligent, so as to meet the escalating needs of human financial services.

At present, the Internet and mobile Internet have been fully developed, the existing dividends are slowly disappearing, the wave of new technologies is still in the brewing and embryonic stage, there is no broad consensus and large-scale application, and personal privacy awareness is gradually awakening... Under the following complex environment, for the emerging technology and application of distributed Finance (blockchain digital currency), which happens to appear, How to make visible progress in the short term and fit in with the development trend of financial services in the future is a problem that needs to be considered in the application development of blockchain digital currency scenario.

Coinone believes that no matter the existing financial services and

businesses, or the digital financial services that will grow in the future, with the development of digital life and the wave of digital economy, their business form, service mode and user needs will change slowly but greatly. Even more profound than the changes in finance during the wave of electronization and informatization.

Due to its integrated underlying technology and its open and inclusive technical concept, blockchain digital currency has distinct advantages over the traditional model in terms of transparency, openness, review, efficiency improvement and cost reduction in some scenarios. We believe that the main opportunities of blockchain digital currency in the future lie in two aspects:

• distributed improvement and upgrading of existing financial businesses or services. With the development of society, some existing financial services and businesses will give birth to the needs of upgrading and transformation. In some cases, it is easier to meet the upgrading requirements by using blockchain technology. By using its characteristics of co construction trust, transparency, openness and tamperability, it is easier to use traditional centralized technology.

• become a distributed infrastructure support under emerging financial scenarios and needs. The deepening of the digital process will

inevitably create many new needs and application scenarios. Their needs for financial services and functions will be urgent but different. Blockchain technology has the advantage of natural fit to the digital scene. Blockchain digital currency based on blockchain technology is fully capable of becoming the underlying financial infrastructure in the era of digitization and Internet of things.

There is no doubt that at this time, we are in a time period of change. The development of Internet, cloud computing, big data and artificial intelligence information technology enables informatization and digitization to reach all aspects of society. The digitization of the real world and the increase of digital virtual scenes also continue to give birth to the financial needs of the new situation. Its scenarios and requirements have the following characteristics:

1) Focus on users rather than institutions

Different from the traditional financial business, which is usually carried out around institutions and among financial institutions, in the new financial scenario, the protagonist is transferred from institutions to end users. The initiation, participation and leading role of all financial acts are transferred to ordinary users. Scenarios are built around end-users, risk control makes decisions around the portrait of end-users,

and business processes are optimized around the needs of end-users...
Under the new financial scenario, the role of institutions is still very
important, but the whole center of the scenario has undoubtedly shifted
to users. Loosely speaking, those who get users in the new financial era
get the world.

2) Online behavior is far more than offline behavior

The traditional scenario revolves around the business personnel of
financial institutions such as offline business hall and customer manager,
and offline payment. It only carries out data informatization and data
transmission and storage through network and computing. The overall
process backbone is still offline. In the new financial scenario, the main
processes have been basically online, and the online proportion of
financial behavior triggering and flow interaction in the scenario is much
higher than that offline. Offline behavior participation is usually only in
some cases involving offline delivery and offline risk control.

3) Financial behavior participants are decentralized and weakly
related

Another feature brought by the online financial behavior is that the
participants in the financial scene have broken the geographical
restrictions of the traditional financial scene, and the participants

involved are becoming more and more scattered and unfamiliar; The proportion of financial behavior Association for the first time or low frequency is higher and higher. This new financial scenario, which is different from the situation that most participants in the traditional financial scenario are strongly related, is becoming more and more weakly related, which brings greater challenges to business collaboration and joint risk control.

4) Digital assets are increasingly involved

The purchase of virtual rights and interests, the protection and circulation of digital asset value, and even the participation of digital currency are more and more in the new financial scene. Most of the scenes in the future will also focus on digital assets.

Distributed finance based on blockchain technology, its underlying technology and applicable scenarios are just in line with the new financial scenario: integrated technology is in line with user-centered applications, the concept based on de trust hypothesis is in line with the characteristics of weakly related participants, is naturally more suitable for online digital virtual scenarios, and supports digital asset related applications... That's why, The unfolding new financial era will be a huge opportunity for the blockchain digital currency application supported by

the Coinone financial ecosystem!

2 Coinone introduction

2.1 What is Coinone

Coinone is a decentralized futures trading platform based on the development of blockchain. It is jointly developed by top technicians in the blockchain digital currency ecology all over the world. It is committed to the application research and development project of blockchain digital currency ecology. Coinone will focus on integrating multiple functions into the Coinone platform to build a platform that embodies the basic values of blockchain, namely compliance, safety, speed An understandable and credible financial ecosystem.

The structural feature of the current securities and futures market is that it needs authoritative third-party institutions, information intermediaries or central counterparties as guarantees to help market participants realize the value exchange of assets and interests. As an interdisciplinary innovation paradigm, with the help of its multi-party consensus mechanism, tamper proof and other characteristics,

blockchain can realize the transformation of the network from centralized trust to weak centralization and multi centralization, and can also improve the efficiency of "transaction is clearing".

Coinone defines and implements a new scheme of blockchain technology, which adopts a new professional futures financial payment system theory, realizes a new definition scheme of decentralized futures trading platform through Coinone, and creates a new model of blockchain digital currency ecology.

With the help of blockchain technology, build an OTC trading platform, as shown in the figure, which can connect a large number of scattered customer resources in various markets. As long as the buyer and the seller analyze the ledger transaction data on the node, they can query the performance information and lock the trading opportunities.
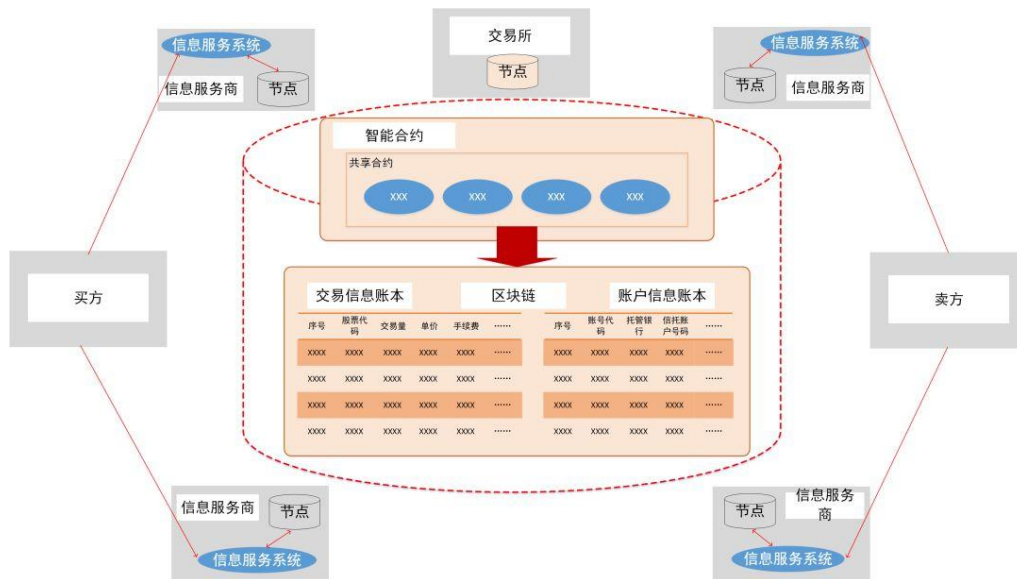
Schematic diagram of OTC trading system based on blockchain

With the help of the smart contract on the OTC trading platform of the blockchain, institutions can broadcast the whole network when there is an inquiry demand, and can also obtain the transaction quotation on the blockchain in real time, which can be executed automatically according to the conditions agreed in the contract; When the credit risk value of the counterparty calculated by the smart contract reaches the early warning line, it will automatically alarm the relevant institutions involved in the transaction.

Coinone establishes a digital currency circulation ecology based on the transparent, safe and efficient distributed characteristics of blockchain digital currency blockchain technology. With the help of

blockchain digital currency platform, block payment technology, unique incentive system and the distributed service architecture of exclusive smart contract, it has become a blockchain digital currency contract with deep scalability.

The mission of Coinone is to establish a value Internet system circulating in the whole scene. The model designed by Coinone platform enables the connection between the chain and the chain. By setting up a series of trusted data sources, the application can start the smart contract and smart application on the chain after a specific event in reality. By setting the threshold value, the application can specify that the smart contract is executed only on a small number of nodes, which greatly saves the computing power of the whole network. It can also specify a small number of nodes for the transmission and storage of main data, which makes it possible for blockchain application scenarios such as digital money and finance.

Coinone will provide a solution so that transaction transfers can be completed almost instantaneously, and digital assets can be issued using the value of anchored currency and anchored specific commodities. Coinone mechanism is the first mechanism to develop internal and external two-way circulation and promote blood circulation in blockchain digital currency.

2.2Coinone digital currency financial ecology

The bottom support of Coinone financial ecosystem comes from blockchain digital currency. The Coinone platform aims to form a new ecosystem of developers and users based on blockchain technology through the exploration of the application boundary and technology boundary of blockchain technology, so as to provide grass-roots infrastructure support for the construction of digital currency financial ecosystem. The advantages of the system are as follows:

• open: projects can be stationed on the platform or developed based on the platform;

• convenience: supporting basic services and mature support system;

• Ecology: projects operate independently and cooperate with each other, data security and resource sharing;

• Globalization: open source code is shared globally, and the global business model is mature.

Coinone is not only an application ecosystem, but also a

comprehensive digital asset service platform and global payment system for digital asset management, trading and practical application. It has the remarkable characteristics of high speed, low cost, high security and can effectively resist quantum attacks. It is committed to becoming a global digital value service organization.

Coinone will ensure the relevant requirements of users for various digital asset services in a one-stop way. At the same time, it will integrate a series of behaviors such as finance, transaction, asset circulation and data application into the landing application of Coinone financial ecosystem, so as to build a national blockchain application platform for all walks of life around the world.

The ecological closed-loop ecology of Coinone platform includes but is not limited to: Mining of digital currency, Dao community governance of digital currency, digital currency agreement, digital currency lending platform, digital currency stability currency, distributed storage, distributed homogeneous token, distributed cross chain interworking in Coinone network and various extensions.

At the same time, Coinone has built a blockchain financial underlying system. The underlying basic platform of its financial payment network will provide blockchain support services for the digital

economy, drive the ecosystem construction of Coinone financial ecosystem, integrate industrial assets and efficiently realize the docking service of industry and finance.

2.3 Deposit certificate in the field of Coinone securities and Futures

1. Contract management of futures brokerage business

Futures companies have a strong demand for electronic signing of brokerage and non brokerage businesses. Using blockchain technology to build an electronic contract platform for futures brokerage business helps to combine the life cycle of electronic contract with the characteristics of blockchain, such as multi centralization, non tampering and traceability, open up a series of processes such as identity authentication, contract conclusion, circulation, signing, filing and legal dispute response, and reduce the signing and management cost of futures brokerage business, Improve the signing efficiency and promote the infrastructure construction of the futures industry.

2. Electronization of private equity

At present, the equity of unlisted companies often proves the ownership of assets through agreements, asset certificates or paper securities. Blockchain can replace paper documents as the electronic carrier of private equity, regulate the registration and circulation of such securities, and ensure that there is no possibility of artificial tampering in relevant processes.

In June 2015, NASDAQ established a partnership with blockchain start-up chain chain to issue and transfer private equity using blockchain platform LINQ. In December 2015, NASDAQ reported using LINQ to complete and record the first private equity transaction. The first transaction was conducted for chain, and the private equity was confirmed and recorded digitally.

With the characteristics of blockchain security, transparency, non tampering and easy traceability, NASDAQ has improved the private equity record and its change history, making the equity registration certificate more efficient and credible. Without relying on a third-party public trust institution, start-ups can realize paperless, compliant and standardized securities registration.

3. Other applications

In addition, blockchain has many other applications in the field of

securities and futures. For example, in 2016, the Abu Dhabi Stock Exchange (ADX) released the blockchain voting service; In 2017, Japan stock exchange group (JPX) released the research on using blockchain concept test in KYC (know your customer) process; Many domestic exchanges and market institutions have also successively carried out research on high-performance alliance chain for main board securities bidding trading, block chain application security management, building warehouse receipt system using block chain technology and other topics.

To sum up, the blockchain is reshaping the basic framework of the financial industry, accelerating the innovation and iteration of securities and futures business and products, comprehensively improving the inter institutional efficiency of the capital market before, during and after trading, and promoting the upgrading of the infrastructure of the exchange.

2.4 Digital asset management solutions

Investors will configure a variety of virtual assets. However, only a few mainstream wallets can display real-time prices. It is difficult for

users to fully grasp the asset status. If they want to understand the industry dynamics, view the market and trade, they need to open different clients, and the operation interface has been switched too frequently.

Coinone has developed a fully functional open source wallet. As a platform wallet with good compatibility, Coinone wallet supports users to perform basic operations on all erc-20 tokens. In the future, it will also support a variety of digital assets under different public chains. Users do not need to switch between multiple wallets; The market information accessed in real time covers most encrypted assets, and users can intuitively understand the value and fluctuation of tokens in the wallet interface. As the main functional entity of Coinone, Coinone wallet is equipped with digital asset intelligent sales contract and transaction function interface. Users can use information, investment and transaction functions in the wallet and enjoy convenient and fast one-stop digital asset services.

Coinone wallet has good compatibility and can connect multiple mainstream public chains, such as eth, BTC, Neo, qtum, etc., which is convenient for users to uniformly manage a variety of encrypted digital assets. Coinone wallet will first support asset management based on Ethereum, and later will be compatible with other types of encrypted

assets.

At the functional level, Coinone wallet supports the display and transfer of Ethereum and Ethereum based tokens, the creation and import of Ethereum wallet, and realizes the most basic management of Ethereum wallet by calling the jsonrpc interface of Ethereum.

In terms of asset display, Coinone wallet optimizes the display content, automatically obtains the prices of most currencies from many mainstream exchanges in the world and weighted average, and displays the asset value and rise and fall range in real time and accurately; Users can also directly view the basic information of tokens in the wallet, such as the rise and fall of issuance time and so on.

2.5 Innovation and advantages of Coinone

The Coinone platform has made a series of innovations in blockchain digital currency blockchain technology and concept, created a perfect blockchain technology system, laid a technical foundation for Coinone to realize world-class full scene circulation, and provided an undifferentiated global digital currency circulation system for billions of users around the world.

1. Unrestricted cross-border transactions

Most legal currencies cannot be freely exchanged or paid across borders, and restrictions on exchange and transfer lead to citizens being unable to invest or consume abroad, which makes the process of immigration, medical treatment, study abroad and even overseas vacation extremely cumbersome. Many countries have foreign exchange quotas for their citizens, have mandatory legal constraints, and are unable to achieve cross-border financial services through third parties. Even in extreme cases, such as when the social environment of the country is experiencing hyperinflation, currency exchange may be completely prohibited, resulting in the inability of legal currency holders to obtain goods and services that may be scarce in their country.

Coinone has successfully developed a unique blockchain technology, which can not only realize the real-time exchange of Coinone for many mainstream digital currencies in the market, buy and sell transactions in major mainstream trading centers around the world, but also successfully connect various mainstream application scenarios online and offline. Any citizen from all over the world can freely hold Coinone for convenient payment and circulation.

Whether it is telephone recharge, real estate rental and sale,

tourism consumption, or oil card recharge and living payment; Or global movie and video theaters and world-famous literary platforms, you can freely use Coinone to pay for consumption. With the characteristics of Coinone blockchain digital currency financial ecology, Coinone breaks through the circulation barriers, realizes unrestricted global transactions, and generates huge profits.

2. Convenient and efficient global transactions

Many widely recognized digital currencies take a long time to create blocks, resulting in slow transaction time. As we all know, the block creation time of bitcoin is about 10 minutes, and even a higher performance digital currency like Ethereum takes about 15 seconds. Cross border transactions in legal currency take longer. Even in countries without cross-border payment restrictions, international payment usually takes up to five working days and the cost is very high, which makes micro payment very impractical. In countries with financial restrictions, they may take longer, spend more, or even be banned altogether.

The currency transaction processing speed of Coinone platform is very fast, usually only a few seconds (less than one second, up to five seconds). Coinone platform currency will be able to support billions of

users without affecting transaction processing time. Different from many virtual currencies including bitcoin, this makes Coinone platform currency a real large-scale trading medium, not just a way to store wealth. In addition, the consensus mechanism of Coinone platform currency allows it to process small amount transactions in parallel at a low cost, making it suitable for payments and transactions of all sizes.

3. Hard currency

Although the mainstream digital currencies in the world, such as bitcoin and Ethernet, are decentralized, the traffic characteristics are obvious and there is no node selection. It is very easy to be blocked by the authorities by limiting the traffic.

Through in-depth research and analysis of relevant international treaties, the Coinone platform uses a series of existing review avoidance technologies, combined with blockchain, flexible use of anti review tools, pluggable transmission protocol, point-to-point network, decentralized nodes, proxy network rotation, network node penetration and other methods to improve the anti review ability, So that the currency of the Coinone platform can not be blocked, so as to improve the connection between the Coinone digital currency and the global Internet, transmit more traffic in China through the use of point-to-point technology, and

reduce the dependence on the global Internet connection.

4. Coinone smart Wallet

The Coinone platform will develop an exclusive Coinone smart wallet in the ecosystem. Users can make more than 100 chain payments and more than 30 traditional payments through the Coinone smart wallet, open up the ports of major exchanges, conduct payment transactions according to the real-time exchange rate, deduct the equivalent Coinone, and achieve second-class transactions and real-time arrival.

one stop management

The unified management of multiple digital currencies through Coinone smart wallet not only supports the storage and management of mainstream assets such as bitcoin and Ethernet, but also supports the standard protocols of smart contract platforms such as Ethereum, achain and kchain, and rapidly increases the tokens issued based on each platform. While reducing the burden of user management, it also provides wallet service support for user blockchain new projects, allowing the project team to focus more on core services.

digital currency financial ecosystem services

Adhering to the core meaning of blockchain, Coinone smart wallet provides users with a decentralized digital currency storage scheme. Wallet keys and address private key information of all types of currencies are stored in the user's local system. At the same time, Coinone smart wallet provides a convenient key backup scheme - users only need to backup once, write down 12 words and save them to a safe place. Even if the types of digital currency are added later, all types of digital currency assets can be recovered with 12 words of backup.

multiple security guarantees

In addition to allowing users to fully control the wallet key, Coinone smart wallet also provides multi signature technical guarantee and two-step authorization verification for digital asset management of different scales. Users can choose mobile phone verification code, fingerprint, living body and other verification methods during transfer transactions to fully ensure the security of digital currency assets.

multi language support

The Coinone smart wallet program will support multiple languages of mainstream digital currency markets such as China, Britain, Japan and South Korea, clearing the language barriers for building world-class wallet applications.

Coinone 平台在区块链数字货币区块链技术和理念上进行了一系列的创新，打造完善的区块链技术体系，为 Coinone 实现世界级全场景流通奠定技术基础，为全球数十亿用户提供无差别的的全球数字货币流通体系。

2.6 Core of Coinone strategic development

1. Aim at the pain point and use it first

As an important financial technology, the research and development of blockchain system should be aimed at futures service business, combined with the pain points and scenarios of futures business. The practical experience of domestic and foreign futures exchanges shows that the characteristics and advantages of futures blockchain can be brought into full play by giving priority to the needs of futures business and studying futures blockchain platforms that meet the functional and non functional needs of their own platforms or futures industry applications, such as futures futures futures trading, private equity trading, settlement, etc.

2. Step by step and verify carefully

Blockchain technology is still immature at this stage. Although

there are many platforms in the market, they are still in the process of evolution and iteration. In 2015, the UK took the lead in launching the "regulatory sandbox" system. Core financial institutions and regulatory authorities can consider building a "financial technology sandbox" with reference to this model.

Carry out POC (proof of concept) verification of innovative technologies such as blockchain in a controlled environment. On the one hand, fintech operators can frequently report to the regulatory authorities and accept review and supervision at any time; On the other hand, regulators and fintech operators can more effectively evaluate the real effect of the new system. It is worth mentioning that POC allows failure, which can avoid greater losses in the next project. From this perspective, POC and sandbox are insurance measures.

3. It is the stone of the mountain, which can attack jade

Core financial institutions such as futures exchanges should adopt an open and inclusive attitude towards innovative financial technologies such as blockchain. Coinone will actively explore the open and shared cooperative research mode, cooperate with professional blockchain technology companies, integrate the technical capabilities of technology companies and the resource data advantages of core institutions, jointly

promote blockchain technology research, and form technology research and application achievements conducive to the safe and efficient development of domestic securities and futures industry.

3 Technical overview

The core of Coinone platform is the combination of the following three characteristics:

- A Turing complete virtual machine (smart contract) with definite resource occupation

- Two way anchored side chain (providing bitcoin denominated transactions)

- A dynamic hybrid collective mining / Federation consensus protocol (for consensus security), and a low latency network (fast payment)

3.1 underlying architecture: big data

While ensuring the services of top-level service systems such as

user storage and payment system, the Coinone platform will continue to build large numbers

According to the system, user trust system and risk control system. Through the continuous optimization of the three underlying systems, we will continue to provide users with safe, convenient and efficient services.

Coinone will collect user data through user behavior and store it in the database for big data analysis and real-time analysis of stream data. Through the analysis of data, guide the Coinone ecosystem to carry out risk control, marketing and operation and maintenance management.

Data acquisition layer

Collect user behavior data, including browsing behavior, click behavior, transaction behavior, evaluation behavior, etc., establish data warehouse and flow data, and provide data support for platform decision-making.

Data analysis layer

The data warehouse will store a large amount of user information and historical data for in-depth analysis; Stream data can be monitored

in real time.

Data application layer   The results of analyzing a large number of data sets can be used in the following three directions:

a. Risk control application

Through the monitoring and analysis of data, you can evaluate the credit risk of the account and reject risk events. For example, when there is a fraudulent account, the system will automatically give a risk prompt.

b. Marketing Application

User portrait   Through a series of users' real data, fit the virtual portrait of users, analyze the motivation characteristics of users' behavior, and realize personalized recommendation and fine operation.

Customer churn analysis and improvement

Analyze the reasons for the loss of users according to big data, find the potential losing users among the existing users, and put forward the user recovery scheme to avoid the loss of users.

c. Operation and maintenance management

Through the peak use of big data analysis platform, reasonably

allocate operation and maintenance resources to ensure smooth use of users.

3.2 Coinone trust system

In order to ensure that users enjoy high-quality products and services on the Coinone platform, Coinone will continue to improve the trust system to improve service standards.

■ **Real name authentication**

All Coinone cooperative suppliers need real name certification and provide relevant business licenses, business entities and other real information.

Coinone will review the merchant information, establish the registration file, and verify and update it regularly.

■ **Evaluation mechanism**

Coinone sets up a user evaluation mechanism to allow users to participate in the supervision of the payment system and solve the problems of asymmetric commodity information and inadequate

merchant services.

■ **Arbitration mechanism**

When there is a dispute between the merchant and the user and the two parties cannot reach a settlement, they can apply for Coinone arbitration. The arbitrators selected by the platform will judge to ensure the legitimate determination of interests.

■ **Elimination mechanism**

In order to ensure the quality of Coinone merchants, merchants with low evaluation score and refund rate exceeding a certain proportion will be eliminated in a certain period.

■ **Selection and certification**

In addition to the quality inspection report of the commodity itself, Coinone, as a third-party organization, carries out quality inspection on the on-line commodities and gives "selection certification" for products with high quality and high price, so as to help users buy high-quality commodities and reduce decision-making costs.

■ **Risk control system**

Coinone will comprehensively build its own risk control system

through risk governance, risk management mechanism and underlying technical support. Carry out quantitative scoring for potential risks, realize risk rating, find out risk management solutions, and improve the defects of bank risk management. In addition, Coinone will provide users with risk control services from the aspects of asset return qualitative indicators, various risk identification and evaluation, internal control environment, control activities, supervision, evaluation and correction.

3.3 Turing complete virtual machine

The virtual machine of Coinone is the core of intelligent contract platform. Smart contracts are automatically executed by a high proportion of network nodes. Smart contracts can be used to process information between contracts, create capital transactions and change the storage status in contracts. The virtual machine operation code is compatible with Ethereum virtual machine, making Ethereum contracts perfectly compatible on Coinone. In the first version, virtual machines were executed by interpretation. In the next version, the plan will be communicated

The opcode is dynamically redirected to be compatible with Ethereum virtual machine using Java bytecode, and the security and memory constraints are strengthened to form a new version of Coinone virtual machine. This will give Coinone virtual execution performance close to local code.

It has the following characteristics:

• Independent virtual machine, but operation code compatible with Ethereum virtual machine.

• Coinone provides Ethereum users with the ability to run their projects on the bitcoin network to enjoy the security of the bitcoin network.

• New computational power opcodes and better real-time compilation provide higher performance.

3.4 dynamic collective mining / Federation

Dynamic hybrid merged mining / Federation is the only low-cost consensus mechanism to prevent the tampering of the blockchain. Other consensus mechanisms have the disadvantage that they do not

need to consume real valuable resources to mine, which depends on reputation and prevents anonymous participation in mining. Other consensus mechanisms also require new entrants to trust some existing participants and find verified and confirmed account books.

The workload with high computing power is proved to be based on periodic burst blocks and requires a low isolated block rate, which requires miners to stop computing when they find new blocks in the whole network and start mining at the head of the new blockchain again. This will lead to the time difference in mining, or the delay caused by the midway switching of the network. This time difference reduces the mining efficiency of bitcoin, even if only a few milliseconds are wasted. Therefore, Coinone uses Decor + block reward sharing scheme to reduce competition and allow miners to delay switching to the best block of Coinone. If a Coinone block is dug when miners switch the computing power of mining machines, they will receive a complete Coinone block reward. If they delay the handover and are still mining at the head of the old blockchain, they will create an uncle block and get a block reward to share. In this way, in any case, miners will not be lost by all isolated blocks, because D É cor + will pay rewards to Uncle blocks, and will also give rewards to the normal blocks of Uncle blocks that comply with ghost rules and the blocks that ensure the security of

blockchain. So as to maximize the mining efficiency of bitcoin.

Because we expect that the computing power of Coinone in the early stage will be less than half of that of bitcoin in the whole network. This may lead to the remaining computing power to launch 51% attack on Coinone to launch double flower attack. To prevent this attack, Coinone miners use workload to prove that mining will include a federated checkpoint. Federal checkpoints are composed of registered federal members and customers who jointly sign to determine the best blockchain status. In addition, Coinone has the last reservation agreement. When the computing power of Coinone is less than 5% of the computing power of bitcoin, the Federation will create blocks. By default, when the computing power of Coinone exceeds 66% of the computing power of the most difficult block on the bitcoin chain and the average block handling fee is higher than the bitcoin block reward, the client will stop using the federal checkpoint, When the Coinone platform is launched, a federation of well-known and respected members of the community will be established. Each member uses the public key to sign the checkpoint scheme. The Federation can add or remove members who use and embed voting systems, but these actions will require a high percentage of members to vote.

The collective mining of Coinone network will encourage miners to

create Coinone blocks. When Coinone still lacks computing power to collectively mine, the Federation will provide security for the network.

Main features:

Mature mining reward. 1-day maturity for mining reward Federal member checkpoint.

Embed checkpoints in transition code.

For bitcoin miners, collective mining will not bring any loss (the loss of immediate switching in the middle state is less than 0.1%, and the delay is close to 0%)

3.5 Fast payment and low latency network

Coinone aims to build a better payment network. In order to achieve rapid payment, several methods have been developed:

Use free competitive blockchains (e.g. hyperledger, ripple, closed loop)

Use hub and spoke networks (such as bitcoin's lightning network)

High POW block rates with high workload

The central radiation network needs a new central node and a new complete wallet client, which is a completely different payment mode. Although this form can be easily implemented on Coinone, it is not a local fast payment system. Coinone complies with Decor + and fastblock5 protocols, which can achieve an average block out time of 10 seconds and will not lead to mining centralization. This is a free and independent mining and incentive policy.　Main features:

• An average of 10 seconds.

• Two stage block transfer (2sbp) protocol.

• Push lost transaction (PMT) protocol.

• finally, the whole network broadcast of competitive blocks to prevent self mining and reduce the stale block rate.

• delayed transactions include heuristics (DTI). The transaction delay of 5 seconds allows the fastest block to be added for confirmation, because the transaction already exists in the memory pool of each node.

• use new network commands to propagate block headers with time priority.

• immediately after the block header information is broadcast, use the new network command to propagate the block transaction Hash list.

• mining on heuristic unconfirmed blocks (mub). Miners can use the 5-second return method to dig in the area with incomplete transaction confirmation. (translator's note: the translation may be inaccurate. The original text is: Mining over block headers with unverified transactions with a 5 seconds fallback.)

• the block header information of the block without transaction will be marked (the transaction here does not include Coinone reward) • each connection protocol is equipped with two prioritized streams for each connection protocol (2psc) The new information transport layer uses information slicing technology, which allows two parallel sessions to use different priorities. This allows the block header information to be sent in a higher priority session and can interrupt the information of any low priority session being transmitted.

• local routing optimization protocol (LRO). Locally optimized block routing is based on peer-to-peer priority. Locally optimized transaction routing is based on priority. (Local Route Optimization Protocol (LRO). Local optimal block routing based on peer priorities. Local optimal transaction routing based on peer priorities.)

• share block rewards among competing blocks using Decor + protocol. Use ghost protocol for chain weighting

3.6 Calculation of side chain

In Coinone, the computing side chain (CSC) has a DSC like structure, which also includes block headers, transaction sets, Coinone network contracts and data allocation through hash links. The transaction still uses the Merkle tree structure. The client sends a computing request to the network, which is propagated through the network. Each miner uses the computational side chain (CSC) to obtain the task. When a task is completed, the working miner will send a confirmation to the computing side chain (CSC) to update the task status and get a reward.
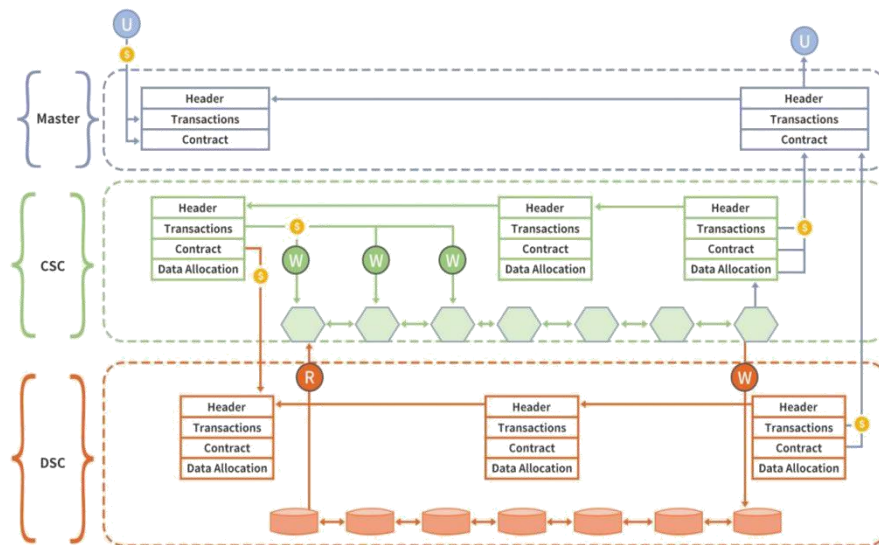
Calculation side chain overview

The solver and verifier in the computing side chain (CSC) will load the code and data into the Coinone virtual machine (DVM) and execute the code in the Coinone virtual machine (DVM). These codes include parallel computing tasks and verification tasks. The miner who calculates the side chain (CSC) needs:

check the format of the block;

check the deduction, and the deposit is valid;

check whether the data and codes related to the task are valid;

if necessary, verify the task results;

read / write data from DSC if necessary;

summarize transactions and send them back to the main chain;

3.7 Ring signature technology

$$\mathrm{Dec}_{sk_s}(E_\sigma(v) \oplus v_s)$$
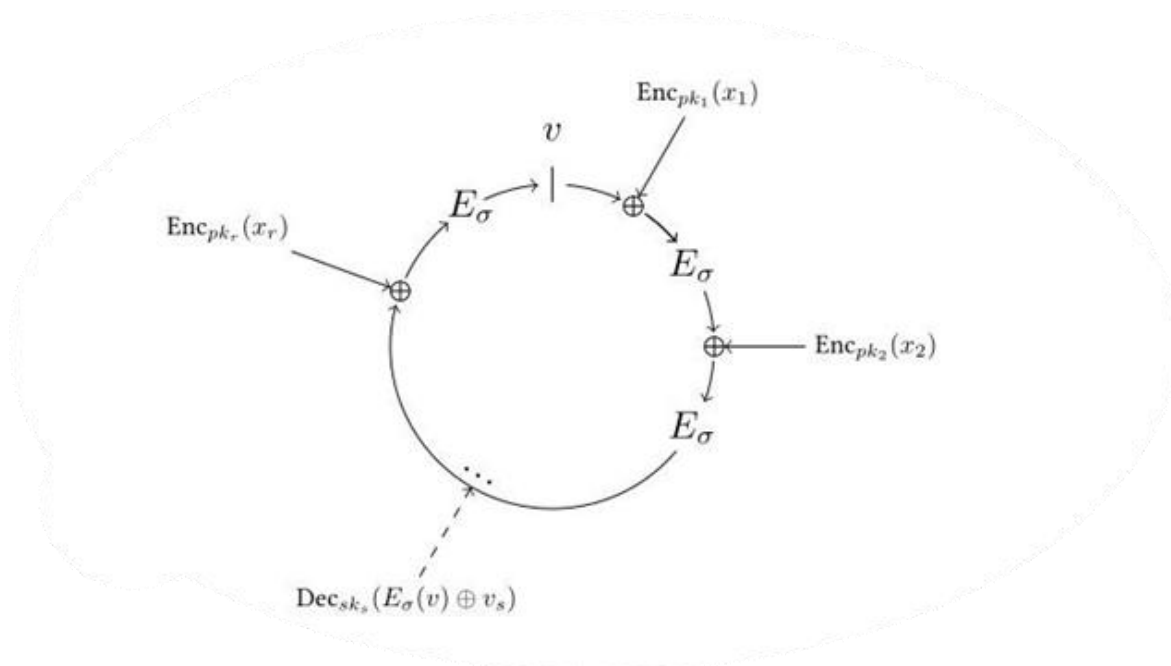
Ring signature refers to hiding the public key with its own private key among n public keys. The specific application is to hide the transaction sender (address / public key) on the blockchain.

Ring signature is a kind of digital signature, which can be executed by any member of a group of users who have a key. Therefore, the message signed with ring signature is signed by someone in a specific group, but it is impossible to deduce which member completes the signature: a security attribute of ring signature is that it is impossible to determine which group member's key is used for signature by

calculation.

3.8 Push lost transmission protocol (PMT)

Considering that each node stores the hash of transactions, and the nodes will inform each other of these transactions, and the miners will immediately package the lost transactions in their memory pool into blocks. This makes it unnecessary for the secondary communication to supplement the lost transaction. Sending the lost transactions before the node requests to resend them is the third stage of 2sbp protocol.

3.9 Delayed transmission transaction packet test (DTI)

The miner will only pack the deals he received a few seconds ago. This ensures with a high probability that the transaction will be received by the miners before the block is excavated. Considering that delayed trading is the favorite of miners, because it can reduce the verification time of blocks and reduce the opportunity to compete for blocks. When the mining on unverified blocks heuristic (mub) is effective on the network, this optimal combination is not required.

4 Coinone token issuance planning

4.1 Introduction to Coinone token

In the future, Coinone token will issue a network currency based on point-to-point technology, which has the same implementation principle in technology. Its creation and transfer are based on an open-source encryption protocol and issued according to the platform without being managed by any central organization.

Issue Name: Coinone

Token attribute: platform currency

Total issued: 100000000 pieces

Distribution mechanism:

70%: used to sign in for free mining output, including mobile mining, behavioral mining, trust and ecological construction

30%: used for native tokens, phased delivery, and rewards for marketing team operation and technical team.

4.2 Coinone Token issuance planning

The whole Coinone token issuance is divided into three parts: ido-lbp-dex, which adopts multi platform, multi chain and multi form:

● **Ido stage**

Coinone token will be issued synchronously on 2-3 Ido (initial DEX offering) platforms, including ERC 20 and heco. Investors participating in Ido need to conduct white list authentication in advance on the platform. The list of IDO platforms and participating tutorials will be published in official channels in advance. Please keep an eye on it.

● **LBP stage**

Coinone token will be configured to the balancer's liquidity bootstrapping pool (LBP). After opening LBP, investors will be able to buy Coinone token. This round is for all investors. Investors participating in LBP do not need white list authentication. The address of LBP pool will be announced in the official channel in advance. Please keep an eye on it.

Note: LBP is a variant of Dutch auction and reverse auction. At the

beginning, Coinone token is set to a higher price. In the case of no purchase, Coinone token price will decrease over time. Please be familiar with the principles of auction.

- **Launch DEX**

Launch DEX and receiving Coinone token will be opened after the LBP is completed. Investors will be free to trade at that time, and Coinone token will be completely priced by the market.

4.3 Future value of Coinone Token

the future circulation value of Coinone token is reflected in the following aspects:

1. Platform ecological circulation

Based on the Coinone platform, many entity applications will be derived. Coinone token can realize the exchange with all digital currencies such as BTC, ETH, usdt and EOS, and support the circulation and payment of all links in the ecosystem, such as collection and payment, transfer, legal currency transaction, currency charging, currency withdrawal, currency voting, sto gateway, crowdfunding,

financial management, public welfare, games, shopping malls and other transactions, as well as legal currency settlement with countries all over the world.

2. Financial transaction payment

Users can use Coinone token to pay for financial transactions, including all kinds of investment and financial management, securities and Futures and other financial transactions. At the same time, it can also be used as a basic means of cross-border payment. So as to bring more benefits to yourself.

3. Credit financing

Users can use Coinone token to establish contact between credit financing participants such as banking institutions, and record enterprise subject qualification, multi frequency transaction information, capital flow information, etc. through blockchain, so that both enterprises and banks can share real and reliable information openly, transparently and safely. For large enterprises, banks can enrich the financing risk control model, reduce the workload of offline manual collection and confirmation of information authenticity, and carry out financing services under real estate evaluation. For the upstream and downstream small and medium-sized enterprises in the supply chain

with financing difficulties, they can obtain credit endorsement based on the subject qualification certification provided by the blockchain and the multi frequency transaction information certification with large enterprises, so as to alleviate the financing problems. As the main body of trade financing, Coinone token can realize barrier free exchange with global mainstream legal currencies and realize more convenient trade financing function.

4. Generality

Coinone token can adapt to diversified business needs and meet cross business financial data sharing, which means that Coinone has enough universality and standards for data recording methods, can represent all kinds of structured and unstructured information, and can meet the cross chain requirements required with the expansion of business scope. This provides a value basis for the universality of Coinone token. So that Coinone token can circulate more calmly in various financial transaction scenarios around the world.

5. Team Introduction

5.1　Coinone Foundation

The Coinone foundation has a complete and outstanding team. The foundation has more than 50 years of global investment management experience and more than 20 years of entrepreneurial team incubation experience. In 2002, it took the blockchain market as the strategic market of the foundation, proficient in blockchain finance, financial technology, Internet Finance and other emerging industries, and has strong and complete business planning and investment management capabilities.

In 2021, Coinone foundation officially launched the company's independently developed digital currency financial transaction infrastructure based on blockchain digital currency - Coinone ecosystem. The Coinone ecosystem realizes the integration of public and private chains, opens up the underlying framework of the blockchain of real-world assets and digital assets, and the Coinone foundation has invested a lot of research funds. Through the R & D achievements obtained through long-term scientific and technological research, the application scenario integration (platform, private chain, alliance chain application integration), the legal effectiveness of smart contracts and other original features, Having the ability of real-world asset digitization

and value circulation is the only choice for building blockchain applications.

Since the project of Coinone was raised and verified, it has undergone many technical modifications and evolution. In this process, it has received input and assistance from professional technology and investors from the United States, China, Singapore and Canada.

5.2   core team

Algernon is a capital market expert with rich operating experience in banking, investment and listed companies. He is a leader in blockchain and digital currency industry. Internet companies with ownership have in-depth research and funding for Internet, blockchain and other industries.

CCO - Christopher Durand, MBA from Laurier University in Canada, once served as the investment manager of Xianda financial group in Canada and the investment manager of Shenzhen Yingxin venture capital company. He has more than 25 years of experience in fund management at home and abroad, is familiar with the global securities market and investment products, and has a solid foundation in economic theory and mathematical Valuation Modeling, Deep insight into global market linkage. Christopher Durand believes in value investment, has a conservative and stable investment style, has a deep understanding of Hong Kong stock TMT, consumer electronics, insurance, medicine, education and other industries, and is a stock selection expert in relevant industries.

The chief technology officer, Agrario Rodr í guezp é rez, is the chief technology officer of Coinone. He has 17 years of experience in the

Internet industry, is proficient in a variety of computer languages, is good at long-term high volume and concurrent available architecture design, and has rich experience in R & D management. Product director Simon Mao, former product business director of Wanxiang blockchain laboratory, is responsible for the design of blockchain product application framework, focusing on traceability, logistics, energy and supply chain finance. He used to be the senior consultant of distributed energy of Fortune 500 companies and the co-founder of an Internet of things enterprise. Specializing in the research of distributed governance model and blockchain product application framework.

Chief operating officer - Stanley Thompson, who has more than ten years of experience in project management, business operation and venture capital. Be good at analyzing the market environment and optimizing the operation strategy.

Theodore, a technical engineer, graduated from the computer department of Yale University and obtained a doctorate in computer and big data. He is an architect, database expert and the chief technical expert of the exchange. He has long been engaged in the development of database application, data warehouse, big data and blockchain in the trading industry and has rich experience in blockchain project development.

6. Development planning

6.1 Initial planning

- Complete the initial design work and project preparation of

Coinone platform, and preheat the online plan.

- open the platform, attract popularity, gather more users, expand popularity and improve recognition;

- in 2022, it will be publicized globally and the initial liquidity alliance will be established

6.2 Medium term planning

- Release multi-dimensional, high-intensity and multiple rounds of reward activities to maintain the popularity

- Develop partners to promote token liquidity and promote the circulation of platform futures trading market

- Regional marketing and public relations activities, complete the global publicity and upgrading, and jointly promote the main home page of major exchanges, so as to greatly improve the popularity.

- Build a global trading community of blockchain digital currency, contact major enterprises around the world and establish

strategic cooperation.

6.3 Post planning

- The Coinone platform will hold the global digital currency summit, establish a global ecosystem, and implement the implementation and application of blockchain digital currency platform technology.

- Jointly launch 60 global centralized exchanges and go global in an all-round way

- With strategic industries as the core, layout the financial payment format of the whole scene of blockchain digital currency, and take this as the basis to extend and build more application scenarios.

7. Risk warning

Systemic risk: refers to the possible changes in returns caused by overall common factors, which affect the returns of all securities in the same way. In the market risk, if the overall value of the digital asset

market is overestimated, the investment risk will increase. Participants may expect the growth of token public offering project to be too high, but these high expectations may not be realized. At the same time, systemic risk also includes a series of force majeure factors, including but not limited to natural disasters, large-scale failure of computer networks worldwide, political unrest, etc.

Risk of lack of Supervision: digital asset trading, including Coinone, is highly uncertain. Due to the lack of strong supervision in the field of digital asset trading, there are risks of sharp rise and fall of electronic tokens and manipulation by makers. If individual participants lack experience after entering the market, they may be difficult to resist the asset impact and psychological pressure caused by market instability. Although academic experts and official media sometimes give suggestions on cautious participation, there are no written regulatory methods and provisions, so it is difficult to effectively avoid this risk at present. Risk of regulatory introduction: it is undeniable that regulatory regulations will be issued around the world in the foreseeable future Bundle standardizes the field of blockchain and electronic tokens. If the regulatory body regulates the field, the tokens purchased during the public offering of token may be affected, including but not limited to fluctuations or restrictions in price and marketability.

Inter team risk: at present, there are many teams and projects in the blockchain technology field, the competition is very fierce, and there is strong market competition and project operation pressure. Whether the Coinone project can break through among many excellent projects has been widely recognized. It is not only linked to its own team ability and vision planning, but also affected by many competitors and even oligarchs in the market. During this period, it may face vicious competition.

Intra team risks: the Coinone team has gathered a talent team with both vitality and strength, attracting senior practitioners in the blockchain field and experienced technical developers. As a leader in blockchain technology, the stability and cohesion within the team are crucial to the overall development of Coinone. In the future development, the possibility of negative impact on the whole project caused by the departure of core personnel and conflict within the team cannot be ruled out.

Project planning and marketing risks: the founding team will spare no effort to achieve the development goals proposed in the white paper and expand the growth space of the project. At present, Coinone has a very mature business model analysis. However, in view of the unforeseen factors in the overall development trend of the industry, the existing

business model and overall planning ideas can not be well consistent with the market demand, resulting in the consequences that it is difficult to make considerable profits. At the same time, as this white paper may be adjusted with the update of project details, the public may not understand the latest progress of the project, and the participants or the public may have insufficient understanding of the project due to information asymmetry, thus affecting the follow-up development of the project.

Technical risks of the project: firstly, the project is constructed based on cryptography algorithms, and the rapid development of cryptography is bound to bring potential cracking risks; Secondly, blockchain, distributed ledger, decentralization, different tampering and other technologies support the development of core business, and the Coinone team cannot fully guarantee the implementation of the technology; Thirdly, in the process of project update and adjustment, vulnerabilities may be found, which can be remedied by issuing patches, but the degree of impact caused by vulnerabilities cannot be guaranteed.

Hacker attack and criminal risk: in terms of security, the amount of a single supporter is very small, but the total number is large, which also puts forward high requirements for the security of the project. Electronic

tokens are anonymous and difficult to trace. They are easy to be used by criminals, attacked by hackers, or may involve criminal acts such as illegal asset transfer.

Other risks unknown at present: with the continuous development of blockchain technology and the overall situation of the industry, Coinone may face some unexpected risks. Please fully understand the team background, the overall framework and ideas of the project, reasonably adjust your vision and rationally participate in token crowdfunding before making participation decisions.