# Concealment white paper

Concealm

A purely hidden anonymous Society

Master privacy 2020

# Preamble

After the first private data deal, we all became transparent in front of big data. We human science and technology are constantly improving, the development of science and technology has promoted the progress of society and increased the productivity; From the era of industrial revolution to the era of global Internet, the change of technology has affected the direction of social progress in the future. In this era when the internet connects global information and resources, human beings have never been so close to each other and understand each other. Human beings are going through a higher level of consensus civilization development process, which is the progress of human social civilization. But with the progress of science and technology in a central world, all the resources began to focus on a few people, people are all uncovered to those who control them.

People's daily life of food, clothing, housing and construction of the digital society, stolen by the people sold and achieved great social benefits. Hackers, data leaks and state-backed attacks put the public at risk for personal data security. It is clear that the past systems not only need to

change the network security problem, but also need to strengthen the high protection of users' privacy and data. Many centralized systems exploit user data and abuse personal privacy because their business model is relying on it. It is clear that the world urgently needs a new system that uses different incentives to ensure that users are under core protection.

Directory

# Preface

The right to privacy refers to the personal right that the private life and private information secrets enjoyed by natural persons are protected according to law and not illegally intruded by others, knowing, collecting, utilizing and making public. However, users are always on the verge of being collected, utilized and made public, without any protection. Mention of large technology companies and traditional finance whose interests' conflict with those of the general public. Many intermediate individuals and machine purchases charge large fees but fail to protect end-user data security and provide value. The emergence of blockchain makes many people regard blockchain and encrypted currency as alternatives to the current broken system, which can ensure stability, fairness and more powerful freedom of expression for all.

Block chain technology is attracted by its unique decentralization technology, involving a variety of talents around the world. Countless people are impressed by its charm and want to use it to change the world; Among them, we are a secret organization of world geeks.

We hope to use blockchain technology to build a world where smart contracts replace all centralized organizations. There

is no oppression of the weak by those in power, no racial discrimination, no gap between the rich and the poor; all people get everything through their own giving, giving can be obtained; this is a world without money, without central organization.

Our organization's first step towards the world is to create a social zone where all can speak freely; it is not watched by a centralized world, and no one can spy on personal privacy through smart contracts. Everything here belongs to us!

## I. Project profile

This highly centralized world allows those in power to dig data and gather intelligence directly into the central servers of the U.S. internet company, with nine international giants, including Microsoft, Hu, google, apple and Facebook、Paltalk、YouTube、Skype、AOL. Here is the rule that our geek organization wants to break, the first step in the challenge of a centralized world; we want to create a truly unspoiled communication area —— a purely hidden anonymous social.

### 1.1 Project description

Given the fact that the centralized world is monitoring people without privacy, the world geek group have developed technology in 2015 and eventually develop solutions ——Concealment. both security of people's assets and privacy of information

Concealment is a real implementation of Turing complete intelligent contract privacy protection system. Compared with the existing centralized system, Concealment can not only realize the privacy protection of account information and transaction information, but also realize the privacy protection of Turing's complete intelligent contract input and

output.

## 1.2 Project vision

People's daily life of food, clothing, housing and construction of the digital society, stolen by the people sold and achieved great social benefits. Hackers, data leaks and state-backed attacks put the public at risk for personal data security. It is clear that the past systems not only need to change the network security problem, but also need to strengthen the high protection of users' privacy and data. Many centralized systems exploit user data and abuse personal privacy because their business model is relying on it. It is clear that the world urgently needs a new system that uses different incentives to ensure that users are under core protection. The vision of our organization is to create a system that protects every participant willing to call trust to smart contracts, protecting their privacy, assets and data from theft and embezzlement.

This is the first step for our geek organization to change the world, giving everyone a secret gathering place where there will be no snooping or surveillance. Build an integrated platform that can be used globally. Not only will the

centralization platform eliminate the potential for data regulation and abuse, but it will also provide users with an unparalleled convenience experience beyond data protection.

### 1.3 Blockchain technology

Making and consensus is an important reason why human beings can reproduce so far. As a group with trust as a prerequisite for communication, lack of trust can lead to poor cooperation and lack of transparency can lead to a lack of consensus. With the advent of information globalization, the problem of trust has become the first problem that human civilization needs to solve.

We have to admit that thousands of years of rapid development of human civilization cannot be separated from the support of a central society. But with the progress of social productive forces and the continuous growth of population, the continuous improvement of material needs, the increasing lack of resources; This directly affects the further development of civilization, let us constantly for the present central structure of the world for rational reflection.

Blockchain appears to point out the direction of solving the problem, through technical means to establish code law,

form a non-tampering consensus mechanism, establish a new trust mechanism —— no trust. This is a new technological revolution, trying to solve the bottleneck of the development of modern human civilization with a new perspective, which is a technological revolution worthy of everyone's participation in exploration. Looking back on the ten-year history of block chain, we can see that the impact of block chain technology on society is gradually far-reaching:

Block 1.0

Allowing transactions to be registered between peers, the first board of the blockchain is usually associated with the introduction of bitcoin, the encrypted currency. Record the digital signatures of storage entities (e.g., individuals, cars, etc.), as well as supplementary information such as property relations, events and changes in property relations.

Block 2.0

the second board book of the blockchain supports ethernet's smart contracts, which implement the existing logic in any physical contract payment and condition so that they can last until the contract expires. Smart contracts are self-executing and can respond to specific events and messages. On this basis, it performs operations and transfers assets between parties,

leaving all records and allowing full transparency in audit purposes and regulatory compliance.

Block 3.0

the third board of the blockchain allows users to meet the necessary business requirements in terms of adopting technology, certificate and identity management, encryption management, using data services, and machine learning, monitoring, management, and operation of the platform.

## II. Real dilemmas

### 2.1 Constraints to a central world

The central world has this desire to control everything, and there are frequent data leaks and topic bans on the block chain of decentralization. Other examples: Facebook Cambridge Analytica data leaks exposed 87 million Americans' personal information, and WhatsApp security vulnerabilities led users to be monitored (Falconer, 2019). These data privacy scandals have brought attention to the pitfalls of centralized platforms.

When any online service is free, users become a product in the sense of fact, and their data is sold to advertisers and

targeted for advertising. This "supervised capitalism" has no end to the demand for data, because their business model depends on this basis, and why they believe that traffic is value.

Moreover, because of its uncontrollable server structure, after refusing to comply with the data and information requests of these national authorities, Telegram was banned (Collier,2018) in Russia in April 2018 and Iran in May 2018, respectively. A number of online privacy advocates espouse Telegram, because they strongly refuse to comply with the government's unjust demands on user information. However, the Telegram itself is still a centralized platform, so it will still be affected by malicious hacking attacks and security vulnerabilities, because the single point of failure is inherent in the centralized system. due to the strict regulation of the discussion of encrypted news by the government. this apparent friction on the ability of people to freely discuss cryptocurrency and blockchain technology highlights another flaw in the centralized system - the ability of oppressive governments to review content and stifle freedom of expression.

## 2.2 Cognitive dilemma of blockchain

blockchain technology has so far not been adopted by mainstream audiences because of its complexity and high threshold characteristics. Many of the blockchain applications that currently exist are still unattractive to most people because they are difficult to use and still cannot compete with centralized competitors. Like blockchain, the interests and value proposition of the Internet is not clear in its early days. Many questions its long-term sustainability, but do not see many ways in which it develops and changes the world.

The Internet was widely misunderstood in the early days, and it was very complex to use and did not fully expand. In general, new technologies often seem daunting and unattractive, so many choose to stick to the status quo. Until the benefits of e-mail are understood, most people choose to post what matters. Misunderstanding and confusion in the emergence of new technologies stem mainly from the lack of education on the added value of these technologies. In addition, early iterations of the Internet are unfriendly to users and are limited to many basic functions, such as web pages and email. The development of web technology and the construction of infrastructure take some time to facilitate the creation of higher-order functions

and processes.

As cryptocurrency has evolved from its infancy to the present, it is often compared to the performance of the Internet in its dawn. It is often misunderstood and cumbersome to use, but has been trying to expand so far. Most people think it is unnecessary and do not see its value proposition and the potential to reshape and develop many industries. Many people are content with the status quo and believe that the cost of switching to distributed systems is incalculable. So people often mistake the current state of technology for its best state.

The crypto world is now in a very fragmented and isolated state, and communities and projects are not closely linked. None of the current cryptographers, project owners and members can exchange cryptocurrency, share insights, discuss trading strategies, and digest the latest lines

Interconnection and unified platform of industry news. On the contrary, those interested in exchange encryption must use a variety of platforms that are centralized communication systems and chat with other like-minded people, and no one can guarantee that their speech and data are absolutely secure.

blockchain cognition, still requires the efforts of each

of our believers.

### 2.3 Technology and hope

The coming of 2020 is not only a new time, but also a new leap in technology. We use distributed blockchain books, and users can safely connect and execute transactions with each other directly without relying on intermediaries or worrying about protecting their privacy. blockchain and decentralized networks provide a self-running approach in a non-trust environment using their distributed books to create transparent, consensus-driven, tamper-proof transaction logs. Each transaction block is verified by the entire network and then unassociated with the chain to provide unparalleled security and accountability.

The use of blockchain and encryption-related languages can be learned by a wider audience and involved in the encryption community through simplification.

Decentralized communications and larger ecosystem solutions will mean that users can safely connect directly to exchange and communicate without worrying about their privacy and will provide an attractive solution for the whole encrypted world to achieve wide adoption. decentralization technology

protects user privacy and data freedom. traditionally, communication platforms rely on centralized servers to obtain information and storage for all data transactions between users. However, in a de-central network like a blockchain, there is no information stored in a central location, which makes it almost impossible for cyber criminals to invade. Hackers and other cyber criminals often infiltrate the entire computer security system and network from anywhere in the world within hours. However, as long as the information is recorded in the distributed ledger of the block chain, it cannot be deleted, changed, relocated or tampered with in any way. attacking a central server is no longer enough to control the entire system. The invariance of this consensus-based decentralized network creates a transparent and secure framework with broad implications.

## III. Technical structure

All of our technologies are designed to create a world of decentralization; the first step is to build a space where we can speak freely, and on this basis, we choose to engage everyone who dreams of decentralization anonymously. Therefore, we look forward to designing a new anonymous blockchain technology that needs to achieve the following objectives:

We best use class methods to provide anonymous mechanisms based on MimbleWimble technology.

With the latest algorithm, our protocol will allow more ordinary users to participate.

our agreement supports multiple assets.

our protocols are well integrated with other existing advanced technologies and systems, such as lightning networks, cross-chain atomic exchanges, and smart contracts. So, it expands the application of this new anonymous currency.

our protocol uses the inverse quantum algorithm to ensure the security of the block chain cryptographic algorithm.

### 3.1 Concealment top-level technical architecture

Concealment the top-level technical architecture, from bottom to top is: data layer, network layer, incentive layer,

consensus layer, contract layer and application layer. Each level can serve a certain application, meet the specific needs of different applications, and help users to quickly and safely implement various application scenarios.

| | | |
|---|---|---|
| **Application** | Intelligent crowdfunding payment clearing | |
| **Contract Level** | Multi-language Intelligent Contract | |
| **Incentive layer** | Incentive mechanism | |
| **Consensus** | POW consensus mechanisms | |
| **Network** | P2P network | Communication mechanisms |
| | Chain Structure | Time stamp Hash |
| **Data layer** | Asymmetric encryption | Cryptographic |

### 3.1.1 Concealment data layer

Besides the standard block puzzle structure, Merkle tree, hash function, asymmetric encryption and time stamp, the data layer also introduces dynamic priority calculation, Fibolacci sequence calculation and cryptographic evidence. At the beginning of the design, the traditional block-stepping structure does not fully consider the expansibility, which leads to the inability to accommodate the large-scale data.

### 3.1.2 Concealment network

Network layer in order to increase network load and speed of network transaction processing, using P2P networking mode, P2P protocol supports data transmission and signaling exchange of each node in block chain network, which is an important communication guarantee reached by data distribution or consensus mechanism. Concealment can use flexible protocols according to different scenarios in system design, support a variety of P2P protocols, in terms of communication security, flexible HTTPS/TLS and other secure communication protocols.

### 3.1.3 Concealment Incentive Layer

Trading is the basic business of changing interests in the Concealment, and any transaction needs to Concealment. eliminated Concealment incentive accounting node in addition to the direct asset income reward, there are accounting contribution reward, accounting contribution reward will become the beneficial basis of re-accounting. Moreover, with the continuous improvement of Concealment technology and ecology, the value of Concealment will continue to improve.

### 3.1.4 Concealment consensus layer

Concealment use the POW mechanism to select nodes and create blocks by holding computing power, and the accounts elected by the community will make decisions on behalf of the community, the decision representatives need to protect the security of the whole block, and if the decision representatives try to use the right to make decisions to tamper with the authenticity of the data, the system will be removed by all users of the community using the DPOW mechanism, and the new community decision representatives will be re-selected, similar to the joint-stock board of directors, DPO W security comes from each user and the algorithm to verify the quality of the node, even if one person has 50% effective voting rights, You can't decide a block alone.

### 3.1.5 Concealment smart contract

smart contracts are the best way to extend blockchain functionality. In the current era, blockchain has many opportunities to combine with traditional industrial applications in many scenarios, but such a combination is far from mature. Smart contracts are solutions that allow us to conduct various experiments at the fastest speed and lowest

cost. Based on the growth of virtual machine technology, we can port intelligent contract technology that supports multiple development languages to Concealment projects and will explore various industries.

After the smart contract is deployed on the chain, in addition to being directly invoked by the user or having access to assets, other smart contracts/built-in native contracts can be invoked or invoked by other smart contracts.

Some functional logic can be implemented in the form of intelligent contracts and deployed on the chain, which is extended by other intelligent contracts as a third-party library.

### 3.1.6 Concealment atomic exchange contract

The actual exchange of the two assets through atomic swaps, a decentralized, non-third-party-free new technology, allows for point-to-point transactions between different types of digital assets without trust, either party complies with the agreement in point-to-point transactions that are completed instantaneously, and the funds are returned to the parties' accounts at the specified time if one party withdraws. Atomic exchange can be modified with a little HTLCs.

In short, using BTC /ETH example, when real-time bitcoin flows from the exchange A to the B of the bitcoin payment channel and the real ethernet B the exchange, the real-time exchange ethernet payment channel A. atomic exchange with special HTLC ensures the atomicity of the exchange: either the exchange is complete or nothing happens.

Payment channel atomic exchange technology is quite novel and has recently been successfully tested between bitcoin and ethernet, bitcoin and Zcash, and bitcoin and wright. Future technology will go further to achieve full compatibility between different HTLC on different chains.

### 3.1.7 Optimistic rollups mechanisms

Optimistic Rollups is a side chain scheme, committed to reducing the burden of the main chain, the greatest benefit of using Rollup solutions is to help users reduce Gas overhead, and this in turn increases the per-second deal able volume (at least a few hundred PS) of the entire network. And the fact that the deal itself is cheaper also means that apps that weren't available because they consumed too much Gas, for example, using complex cryptography, now also become possible to use. Therefore, Although the Rollup programmer itself does not provide privacy benefits, But it is the appropriate basis for

the development of privacy protection technology. Similarly, Rollup the scheme itself does not improve the delay (i.e. the speed of the transaction), But it provides a good environment, Let the state channel, which provides "quasi-real-time certainty ", be developed. Optimistic Rollup methods of processing data also give it good simplicity, compared with other Layer-2 agreements, this conciseness stands out.

### 3.2 Anonymous mechanism

MimbleWimble is an anonymous technique that has proven to be very reliable. With this technology, we can protect the privacy of users on the block chain. Compared with other zero-knowledge proof plans, it is lighter and maintains its security.

the dual-mode depends on elliptic curve cryptography (ECC). in ECC, a large number of k are usually chosen as the private key. k*H as the public key if the H is a point on the elliptic curve. Considering the properties of elliptic curves, it is difficult to derive the private key from the public key k, because the division of curve points is very difficult. Based on this property, we can hide the actual transaction amount in the transaction as follows:

Suppose the transaction volume is v, when the node checks that the output of the transaction is equal to the input, it needs to verify the v1+v2=v3. As shown in the formula below, the two sides of the equation are multiplied by H, point on the elliptical point:

v1*H+v2*H=v3*H, although it becomes very difficult to infer the actual transaction amount in this way, it is still possible for an attacker to infer the value of the v1 because the number set that can be tried is still limited. So we introduce the point G, the second point on the elliptic curve, the private key r. values of any input and output in the transaction are represented by r*G+v*H. r and v. cannot be deduced considering the property of elliptic curve The equations to be validated are as follows:

R1G+V1H+R2G+V2H=R3G and V3H

Also, request r1+r2=r3, so the actual transaction amount will be properly concealed in the actual transaction, the transaction amount is only limited to the transaction parties to use the block chain node to see the information is encrypted number, the private key is only for the user's own use. to verify that the input of the transaction is equal to the output and to protect the sender's private key from being cracked by the

receiver, the sender needs to select a redundant value and add it to its own private key. The receiver can only see the sum of the two and never know the value of the private key that is only available to the user himself. only need to verify that the output of the transaction is equal to the input, only need the trader to know the excess value.

Therefore, excess value is used as the private key of the transaction. validation UT XO can prevent double spending. In the merge process, the verification process is similar in a single transaction, and to verify is that the output is equal to the input, so in the merge (including mixed transactions and removing intermediate states) transaction, the verification is still that the final output is equal to the input in essence. For transactions in intermediate states, simply verify their signature. In the case of dual spending, nodes can easily check that the total transaction output is not equal to input, just like Bitcoin. During the Mimble-wimble, the node can compare all funds from mining with the total amount held to check whether the total money supply is correct. A proof of scope ensures that there is no excessive currency issuance in the transaction.

### 3.3 RandomX mining algorithm

RandomX is a workload proof algorithm for general CPU optimization. RandomX use random code execution as well as several memory techniques to minimize the efficiency advantage of dedicated hardware. RandomX is also named for "random code execution "(random code execution).

Technically, RandomX use virtual machines to perform programs in a particular set of instructions, such as integer operations, floating-point operations, and branch predictions. Such programs can be instantly converted into CPU native machine code, and finally, using the hash function Blake2b merge the output of the executed program into a 256-bit result. RandomX can run in two modes, fast mode requiring 2 GB of shared memory or light mode requiring 256 MB of shared memory. These two modes can be switched at any time, and the results are the same, but the fast mode is suitable for "mining ", and the light mode is more suitable for verifying transactions.

Only two GB of memory and a modern CPU are needed to dig, and the entry threshold for ordinary users to participate in mining has been lowered a lot. If you buy any new one in two- or three-years PC, the memory condition is definitely met. CPU, developers think the post-2011 CPU is more appropriate,

depending on the configuration, and based on some of the data available, AMD seems to have an advantage over Intel. If you want to run a full node, you just need to use "light mode ". The memory requirement is only 256 MB.

mining algorithms are part of the consensus. Here, we choose the RandomX mining algorithm against AS IC. Using this algorithm, Users can participate in mining, without a fancy machine, this will provide a fair environment for all participants. At an early stage, no special rigs, CPU is the only unit that can be fairly excavated. At this point, sufficient user involvement can well ensure the dispersion of our protocol. In addition, with different algorithms, we can prevent bad players from attacking Concealment network. RandomX such POW algorithms with ASIC resistance will further enhance the permanent, low-cost and tamper-resistant network we provide. RandomX help us ensure a decentralized content policy in Arweave networks, will maintain a good distribution among the global parties.

### 3.4 Encryption algorithm

The non-interactive zk-SNARKs zero-knowledge proof Celare adopts the non-interactive zk-SNARKs zero-knowledge proof system, which aims to completely solve the problem that the transaction is tracked to expose the user's privacy. zk-SNARKs is an encryption method based on pure mathematical theory, and like the essence of block chain, the advantage of this way is that it has a wide range of application scenarios by using it without relying on external operating environment. the basic meaning of it is "zero knowledge Succinct Non-interactive Argument of Knowledge", look at their meanings separately :• zero knowledge： zero knowledge, i.e., not revealing any internal information in the process of proof, as shown in the example above ;231• succinct： concise, mainly means that the verification process does not involve a large amount of data transmission and the verification algorithm is simple; • non-interactive： has no interaction.

The two examples given above, while achieving zero-knowledge proof, require multiple interactions between Prover and Verifier to achieve satisfactory reliability, and this technique attempts to completely avoid these interactions. Combined, zk-SNARK is a "technology that proves that I know

what's inside, simple and easy to operate, and the key is that you know nothing about the message or the content of the transaction, except that you can conclude that it's right, so that privacy and anonymity are truly achieved.

Of note, At the time of selecting z k -S N A R K zero - knowledge proof curve, Celare chose the BLS12-381 curve with higher safety factor. B N 1 2 8 curves (Barreto -Naehrigcurves) vs BLS1 2-3 8 The curve (BarretoLynn-Scott curves) is the pairing-friendly elliptic curve, BN128 and BLS 12-381 are still different.

## IV. A new world created by technology

blockchain technology development so far, although there are a lot of imperfections, but it can be seen that all individuals and communities who have faith in blockchain are actively working to promote the healthy development of the industry ecology. A strong cross-chain demand, on the one hand, privacy protection needs, the emergence of Concealment will greatly change the status quo. Privacy protection is a strong demand of both individuals and organizations in the real world. Concealment support Turing complete intelligent contracts, cross-chain asset transactions and various related privacy

protection, can support the expansion of different economic ecology. From the Concealment system, the distribution and control of anonymous assets will no longer be exclusive to a few geek organizations with deep knowledge of cryptography. Ordinary developers, with relevant business needs, can issue their own anonymous assets on the Concealment chain and establish their own privacy ecology, which greatly expands the scope of application of blockchain privacy protection related technology.

### 4.1 Secret social DAPP

As more and more centralized platforms begin to embrace encrypted communities, covert social DAPP is a completely new, decentralized, privacy-preserving chat application that can nurture communities and connect with people around the world without fear of third-party and government censorship. Hidden social DAPP is a safe haven where users can achieve freedom of expression without monitoring and can share data without reservation without being hacked and manipulated. Hidden social DAPP is designed to protect users' information and is the communication and encryption center of the whole world. Hidden social DAPP is the world's first decentralized

mainstream applications including private and group messaging, secure audio and video calls, distributed file storage, in-app multi-currency wallets, intra-chat currency encryption transmission, content publishing, paid media, etc.

Hidden social DAPP establish a new social ecology of decentralization, freedom and equality, decision privacy and social co-governance. Block chain distributed technology makes the user communication information and records completely encrypted, each account needs to be decoded through the user's private key, so that the user's social data is completely owned by themselves.

P2P(point-to-point) privacy social network will cover Facebook & WeChat users in the future, and because of the openness of hidden social DAPP, can intervene in any product and service. seamless access to private social DAPP. for financial services and living services Hidden social DAPP can integrate more services and attract more people. And the traffic brought by the services will also enable the products and service providers, constitute a virtuous circle.

### 4.2 Artificial intelligence

The fusion of AI and blockchain is now more at the data

level, and AI need data to train. Over the past two years, blockchain projects have used Token to motivate people to contribute data. However, the data AI need, especially for special industries, are sensitive data, Concealment the protection of privacy data will have great application value, which is helpful for AI to process data. Furthermore, the convergence of blockchain and IoT technologies is promising, for example, future smart terminals will be different, not only to complete similar actions to pay for electricity, because smart devices themselves also produce data, so when others use its data, this cost is not necessarily money, it may be a value measure mutually agreed between the demand side and the supply side, but it can be determined that this value measure is difficult to be reflected through the existing legal currency, and Concealment can fill the gap in this area.

### 4.3 Health

data privacy is embodied in all aspects in the medical and health related industries. from individual cases to medical records, the multi-color-oriented privacy protection and authorization mechanism requires very flexible and secure privacy protection capabilities. it involves hospitals,

patients, insurance companies, pharmaceutical companies, etc. the protection of data privacy and the restriction of authorized use are particularly important. Concealment systems that address privacy issues for patients and hospitals also open channels for insurance and pharmaceutical companies to be safe and compliant and to use relevant data with patient permission.

### 4.4 Advertising in the chain

According to PricewaterhouseCoopers , 2015 is the last year for companies to invest more in traditional advertising (newspapers, television, etc.). Digital advertising has accounted for more than 50% of the market since 2016. The digital advertising market is growing rapidly and blockchain technology can help improve transparency and efficiency

Now we have many middlemen in the process of advertising purchase: bidding platform, demand side platform, publisher. This makes the traditional advertising industry has the complex process of advertising purchase, expensive, advertising fraud and other difficult problems to solve.

Advertising alliances use blockchain distributed technology and provide advertisers with greater transparency,

thus clarifying which participants each transaction involves, and seamlessly coordinating data and finance. At the same time, the media planning, media purchase and tracking and analysis services will improve efficiency, reduce advertising publishing costs, achieve precision marketing, blockchain technology will also effectively reduce traffic cheating.

### 4.5 Concealment digital money wallet overview

Concealment digital money wallet is a wallet application that connects digital money and the real world. The card issued at the same time Concealment ,Concealment the digital money wallet supports a variety of card types, including BTC、ETH、BCH、LTC、ETC、ATC、EOS、GXS、USDT nine public chains and many other card types.

Concealment main service carrier is composed of three parts: wallet APP、 digital currency bank card. By Concealment the products and services of the platform, it provides the services for enterprises to rapidly deploy efficient blockchain solutions, while realizing the one-stop management of Bitcoin, Ethernet currency, various tokens and enterprise's own digital tokens, simple and convenient to complete the transaction and exchange of digital currency, and can bind digital assets to

bank cards, realize seamless connection between digital currency and the real world, let your digital currency apply to various transaction consumption scenarios, and truly activate your digital assets. Unique cross-chain and cross-contract technology, combined with its own high-performance public chain → to provide a strong infrastructure for the field of digital money, promote the application and development of digital money.

### 4.6 Concealment public chain ecology

Concealment hidden ecology aims to solve the problems people encounter in the central world, Concealment has unique cross-chain and cross-contract technology, and combines its own high-performance public chain to provide a strong infrastructure for the field of digital money to promote the application and development of digital money.

on the one hand, Concealment provides a safe, convenient and decentralized one-stop management scheme through the support of various blockchain asset types. Concealment users can use mainstream digital currencies such as Bitcoin and Ethernet currency for unified storage, management and exchange transactions, not only can fully control their digital assets,

but also greatly reduce the threshold of digital currency use and management burden, effectively promote the flexible application of digital assets.

For one thing, Concealment has a high-performance blockchain that supports Turing's complete smart contracts. Concealment main chain is a non-Turing complete intelligent contract, which provides secure financial services for digital assets and avoids the huge security risks brought by Turing complete intelligent contract; Concealment also has a one-click customizable side chain, the side chain supports Turing complete intelligent contract, Concealment provides proprietary cross-chain and cross-contract technology to link the main chain and side chain together. Whether contract assets on Concealment or non-Concealment assets can be transferred and exchanged through the technical freedom of Concealment cross-chain and cross-intelligent contracts. Concealment is a block chain for digital asset issuance, exchange, value transfer and other financial attributes. At the same time, it has the function of one-click configuration to generate Turing complete side chain, so that enterprises can concentrate on their own business logic without worrying about the security of digital assets and the high cost and difficulty research and

development of block chain. On the basis of Concealment chain, Concealment platform provides distributed computing power and distributed data interface for digital assets in Concealment ecology, which greatly enriches the practicability of block chain.

On the other hand, Concealment jointly issue digital currency bank cards through cooperation with banks, card issuing institutions (Visa, Master, etc.) and their agencies. Users can apply for virtual or physical bank cards through Concealment online, using any digital currency to recharge the bank card, can be in the world tens of millions of bank card processing outlets online and offline consumption and ATM withdrawals, save users exchange and manage a variety of legal currency trouble, but also greatly expand the application of digital currency scenarios. Concealment Card, any digital assets have a link to the real-world bridge, is no longer floating in the air dream.

## V. Compliance model

### 5.1 What is Concealment (CLT)

Concealment is the name of the basic circulation unit in the secret ecosystem and the only medium of commercial and financial transmission. besides being used for account recording and payment, Concealment can also participate in the ecology of anonymous socializing, motivating the running of the master node (ensuring the stability of the network), and running smart covenant within the system.

### 5.2 Basic information on Concealment (CLT)

**Gross circulation: CLT 1,500,000**

**Form of proof: POW**

**Mining algorithm: CryptoNight**

**Block interval :60 min**

**Block size :≤8 MB**

**Initial single-block production: CLT 500**

**Reduction cycle: Every 2N * 100 block height (N is a positive integer)**

**Reduction: Block rewards halved**

### 5.3 Concealment (CLT) economic model

None of the CLT was obtained by the participants solely through POW proof of work. All CLT accounts will be made public to the holder. CLT issued, the system confirms the adjustment time according to the height of the CLT block. Production was reduced by 10 per 1,000 blocks. Everyone involved in the mining can get the same reward possibility.

## VI. Project planning

With the continuous development of blockchain technology and digital money market, secret ecology as a technology platform will continue to contribute to the transformation of the world. Set up a number of ecological plate applications, opening up a new era of central world history. Taiwan is committed to subvert the traditional central world, build a perfect distributed intelligent comprehensive system, access massive distributed applications in the ecological system, quickly link the vast number of user groups, enable products with traffic, break down platform barriers, reduce economic losses, and optimize the chain of interests.

### 6.1 Initial planning

The first step in the transformation of the world is to create a decentralized, anonymous social DAPP, DAPP has been tested. When the block height reaches 50000, open the first round of public test, any user can participate unconditionally. Anonymous social DAPP, online will also decentralize the wallet. The payment system based on blockchain technology, whether online payment from domestic and foreign e-commerce or transfer remittance from home and abroad, can provide better rates and higher efficiency than the traditional channels, effectively save the transfer remittance between enterprises and users, payment costs and time, and achieve global cross-border payment convenience.

### 6.2 Medium-term plan

If the block height reaches 100000, it will be formally launched Concealment the main network. A crucial step towards the creation of a decentralized world. Anyone who wants to share a common understanding can create their own DAPP. on the main network at the same time, the corresponding chain advertising system, the main network ecological supplement. And, rely on the main network to store information medical test chain officially start testing.

### 6.3 Long-term planning

We will improve the decentralization system and continue to promote; explore in the platform and sub-system to start the artificial intelligence program, and select opportunities, select the type of development to complete the initial version of artificial intelligence, will persevere in the block chain technology, computing power model in depth development. After the completion of the artificial intelligence algorithm upgrade, the formal opening of artificial intelligence block chain era. Through the development of artificial intelligence, intelligent contracts as the law, artificial intelligence as the implementation of the new world.