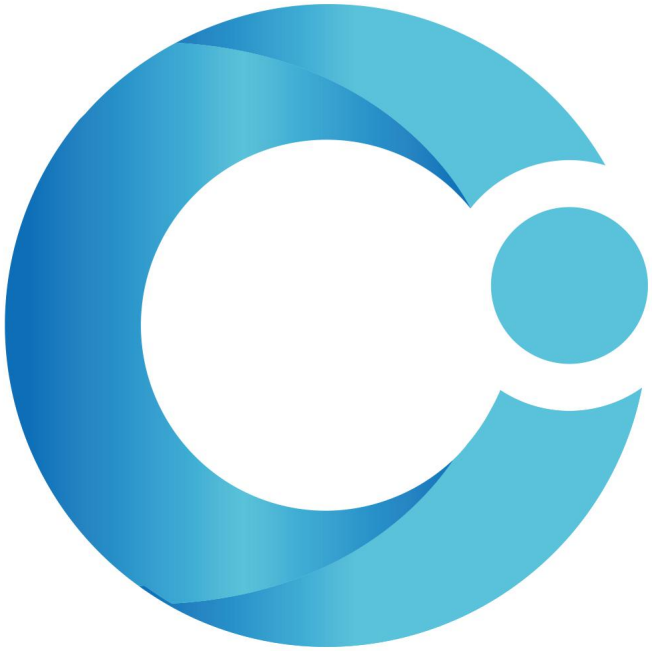


Cryptozoic

CRYPTOZOIC WHITEPAPER

CRYPTOZOIC WHITEPAPER

CRYPTOZOIC WHITEPAPER

INTRODUCTION

In 2009, the world's first decentralized cryptocurrency-bitcoin, was created by the geek guru “Satoshi Nakamoto”. Since then, cryptocurrencies have exploded. Thousands of them have been created and applied in various fields. Cryptocurrencies make decentralized monetary finance possible and have proven to be a new tool for promoting global payments and consumption. Cryptocurrencies are based on blockchain technology and have a decentralized consensus mechanism, subverting the traditional banking and financial system that relies on centralized regulatory system. It makes the financial world free of power and monopoly, and allows all participants to enjoy equal rights and obligations.

Basically, bitcoin is a kind of virtual currency of peer-to-peer (P2P) systems, and the structure formed based on bitcoin payment and circulation transaction is called distributed ledger.No matter where the two parties are currently, the transaction process is safe and efficient. No intermediary is needed. The transaction results are generated directly across regions. With bitcoin, you can send it to anyone in the world at any time and anywhere. Similarly, you can accept bitcoin from anyone in the world.

Ethereum was born and developed on the basis of bitcoin, which is the second largest cryptocurrency system in the world after bitcoin. Ethereum makes innovations and improvements on the basis of bitcoin, introduces a single cryptocurrency system into smart contract technology, and forms an open source public blockchain platform with smart contract functions. Smart contracts are triggering programs running on a decentralized Ethereum Virtual Machine that allow people to process peer-to-peer(P2P) collaborative transactions by writing applications (DApps) based on Ethereum. Ether are cryptocurrencies issued by ethereum that play an active role in maintaining the ecology of ethereum. There are essential differences between ethereum and bitcoin distributed ledger accounting methods. ETH not only supports peer-to-peer(P2P) transfer between users, but also supports the automatic performance of transfer transactions through smart contracts. Smart contracts give automatic transfer and guarantee the fairness of transactions.

Ethereum was proposed by Vitalik Buterin (V god), a talented post-90s Russian programmer inspired by bitcoin, aiming to create "the next generation of cryptocurrency and decentralized application platform".

If bitcoin is just a decentralized system for issuing and circulating cryptocurrencies, ethereum is a distributed operating system with smart contracts. Ethereum not only supports cryptocurrency

accounting, but also supports various decentralized applications. These applications operated in a decentralized environment without the possibility of fraud, censorship, downtime, or third-party interference.

Bitcoin is a store of value that has been developed into a global, peer-to-peer, distributed, transparent cryptocurrency.

Ethereum, by contrast, is designed to provide an ecosystem for distributed applications and decentralized autonomous organizations(DAOs). Contrary to what most people think, ethereum and bitcoin itself have different goals. Ethereum focuses on making blockchain more attractive to users, while bitcoin aims to change the entire financial industry. Both are leaders in their respective niches, but they are not direct competitors.

Bitcoin and ethereum are both based on decentralized blockchain technology, but there are many differences in the deep technology field. As for the specific manifestation of decentralization, bitcoin is mainly divided into three aspects: complete node decentralization, computing power decentralization and development decentralization. By contrast, ethereum's development process is completely centralized, which can greatly improve the efficiency, but also makes it unable to guarantee the safety of its rules and vulnerable to attacks.

Ethereum aims to be a platform, while bitcoin is a monetary system.

The existence of bitcoin threatens the absolute control of the national government over the currency issuance, so the government has the motivation to eliminate bitcoin, which will become one of the biggest obstacles to the sustainable development of bitcoin. Ethereum is not defined as a currency, but as a platform for secondary development. The government has no reason to eliminate ethereum, but wants more people to use its technology. It is strongly recommended that privacy protection and transaction data safety should be exploded and strengthened much more in condition of that securities and properties are in leak.

So we started to think about whether if there is a system which can combine the monetary properties of bitcoin with the smart contracts of ethereum. And also we can build anonymous trading characteristics and anonymous trading features in that system. Therefore the developers over the worldwide can participate and exploit more application areas for decentralized finance in the system while the financial value of cryptocurrencies are infinitely amplified.

We know that the power of finance is great. Finance is the ideological expression of human value.

All conscious human social activities are based on finance. The circulation and transaction of money are only the most basic manifestations of financial activities. A complete financial ecology needs diversified manifestations with multiple scenes implanted to meet various needs. Just as the general monetary policy will also appear such as futures, foreign exchange and other financial commodities, and further develop more financial derivatives.

The diverse inclusiveness shown by ethereum is worth learning from. Therefore, we salute ethereum and bitcoin, which will create a new decentralized, free financial, anonymous trading ecology - Cryptozoic . Let the wealth in the broad financial ecology drive forever, realize the possibility of exponential growth of wealth in various application scenarios.

Cryptozoic derives from the pre-cambrian period of terrestrial history.

Looking back at the history of cryptocurrency and blockchain technology, if we can think about the future of decentralized finance as comprehensively as the Cryptozoic, the world's economy can be promoted. The Cryptozoic pays homage to its predecessors and is also a memory of history, and if time can be turned back, we can look further into the future. Bitcoin has risen more than 2.5 million times since it was launched, which is an unattainable past. People are eager to see the world again. The Cryptozoic defined cryptocurrency finance time tunnel, which will let us review the explosive power of cryptocurrency.

WHO ARE WE?

The Cryptozoic pays tribute to the great pioneer of cryptocurrency finance bitcoin, and to the block chain ecological pioneer Ethereum. Based on the block chain technology, the original dandelion network and the anonymous trading system, we build a new generation of decentralized cryptocurrency financial system.

Cryptozoic mimics the evolutionary history of the earth's surface, the pre-cambrian period of terrestrial history. It is divided into archean, proterozoic and phanerozoic. If bitcoin is compared to the archean phase, ethereum is like the ancient eon phase, and the Cryptozoic project is like the earth entering the phanerozoic phase. Cryptozoic is a symbol, meaning that cryptocurrency finance will enter the next development moment.

Cryptozoic attach great importance to the invisibility of financial business development, and the name echoes the technical characteristics. In terms of technology, in addition to the use of block chain technology to ensure the decentralization of financial transactions, multiple cryptography technology will be used to ensure the hiding of node IP, hiding of transaction address, encryption of key information, etc. All Cryptozoic users can enjoy an absolutely free, secure and anonymous network environment. Every transaction, every element and every frame event on Cryptozoic network can be hidden and protected.

The Cryptozoic has has DApps and operating environment similar to ethereum. The Cryptozoic not only has a decentralized cryptocurrency accounting system beyond bitcoin, but also supports unlimited developers to build broader application scenarios based on Cryptozoic system. Cryptozoic underlying block chain system adopts the same UTXO Mining model as bitcoin, and is equipped with virtual machine program for smart contract writing and execution.

The social network of dandelion is the original value relation network of Cryptozoic. The network is the basis of consensus. The interconnected CAID is the value individual in the dandelion network, and Cryptozoic wealth ecology is made up of these CAID. Meanwhile, the system fission of dandelion network will also increase the wealth of value individual. In order to promote the fission of dandelion network, Cryptozoic ecosystem also contains CAID transmission chain methods such as flying program, exploration program and wanderer program.

The Cryptozoic also innovates the trading mechanism on the basis of cryptocurrency and blockchain. A TWIN trading mechanism called twin-ex is divided into two sections: E2V&V2E.

This trading mechanism can effectively maintain the value of VCC and increase indefinitely.

CRYPTOZOIC BIRTH CONCEPT

Financial attributes dominate wealth freedom!

In today's world, everyone desires wealth and freedom. The Cryptozoic believes that the real freedom of wealth is discretionary wealth on the basis of owning, not restricted by anyone or any organization, can be used in any place, trade with anyone, and can be any form of value transfer.

value owners cannot obtain the real freedom of wealth. The centralized financial system is mixed with centralized monetary management, centralized circulation restrictions, and centralized rules and systems. When wealth accumulates to a certain extent, the owners of wealth will be "imprisoned". In the traditional centralized financial system, wealth is not only a symbol of purchasing power but also social responsibility.

Cryptozoic uses decentralized cryptocurrency to subvert traditional financial attributes, enabling wealth owners to freely control their own wealth without being affected by other factors.

In a traditional financial system, wealth is limited and value is constant. In order to maintain stability, money is also required to be relatively stable in value, but the value of money itself depends on social supply and demand. On the one hand, the supply side needs the cost burden, which keeps out the proles and causes the serious imbalance of wealth distribution. On the other hand, the market supply and demand relations of stable money are all regulated by centralized organizations and lack of value elasticity, which easily leads to inflation and deflation.

Freedom of wealth is freedom of value, not only of the holder, but of the currency itself. The Cryptozoic finance has the property of self-regulation, and we don't need to interfere with it, and its value is completely determined by the supply and demand of the market. We encourage everyone to participate in it, limitlessly spreading like dandelion seeds. The more participants, the greater the demand, the more conducive to the amplification of financial value.

THE GOAL AND VISION OF THE CRYPTOZOIC

Cryptocurrency VCC issued in the Cryptozoic creation block is regarded as the value symbol of the

whole ecology. VCC is a dynamic value, and its market circulation price will be unaffected by any individual or organization, which is more in line with the Cryptozoic freedom concept. The value of VCC completely depends on the size of Cryptozoic ecology. From a microscopic perspective, the price of VCC is determined by the system of dandelion network. The more CAID that joins the dandelion network, the stronger the belief of VCC will be. In the future, VCC-based applications will be more extensive, so the price of VCC will be higher.

Cryptozoic VCC aims to be 100 times of ETH.

Start the third, surpass the second, aim for the first. The reason why we believe that the VCC value can surpass ethereum 100 times is as follows: the goal of Cryptozoic is the benchmarking of ETH value. In order to ensure the propagation of the network and the conservation of VCC value, Cryptozoic has designed excellent wealth increment mode and individual link system. The Cryptozoic market will start unlimited fission.

CRYPTOZOIC KEY ADVANTAGE

Completely decentralized community governance

The operation modol of Cryptozoic is with no foundation or corporate body, and is a completely decentralized project. It relies on community operation and global participation, and is not controlled by any centralized organization. Cryptozoic conception comes from global alliance community and is the product of collective thinking.

Each part of the Cryptozoic is proposed by members of the community independently, and adopted and rejected by voting. Cryptozoic not only achieves decentralization in technology, but also achieves complete decentralization in project initiation and operation.

The strong consensus of dandelion network

Cryptozoic participants (CAID) establish proximity to each other to form a dandelion network, which is not only a social relationship but also a value consensus system. Different from the fission network in the market, it is a three-dimensional social network composed of different source points. Everyone can establish proximity relationship with each other. The relationship between individuals based on the dandelion network makes the consensus stronger.

TWIN-EX value balance mechanism

Except for the resonance trading, Cryptozic first proposed twin-ex trading mechanism, which is an inseparable two-way value anchor between VCC and ethereum, and to make the future circulation value of VCC subjects to natural market regulation.

CAID anonymous authentication mechanism

CAID will be the unique and universal identity of Cryptozoic universe. No matter it is the community ecology, the application of DApp, or the use of exchanges, their authority and qualification will be formed based on CAID authentication.

Privacy technology builds anonymous ecology

Cryptozoic is a chain network system based on block chain distribution ledger. Based on the trusted computing anonymous authentication system, distributed. multi-dimensional anonymous authentication system, distributed data system and other basic modules, the bidirectional anonymous authentication protocol is constructed, and the single and double anonymous authentication of different trust domains is realized to construct a distributed anonymous basic system across chains, industries and terminals.

The world's first anonymous exchange

Cryptozoic community has built an anonymous exchange to realize anonymous transaction withdrawal and currency exchange, so as to ensure that Mining address and personal information are not tracked.

CRYPTOZOIC ISSUANCE NOTES

VCC is based on the creation block issue of Cryptozoic underlying public chain system, without setting the total amount of issue. The issuance quantity is produced in the form of mining according to the market demand. When the market demand shrinks, VCC will be recycled in the form of TWIN—EX. The market dynamic self-adjustment mechanism can ensure that the value of VCC conforms to the current market supply and demand relationship, and neither inflation nor deflation will occur.

Cryptozoic public chainis is also compatible with ethereum. All DApps running on ethereum can run on Cryptozoic, and all cryptocurrencies and DApps issued on ethereum can be compatible with the Cryptozoic privacy and anonymous trading environment.

Distribution: POW+MPOS+Cryper(original consensus)
Account model: UTXO account
Communication: SSL communication
Anonymous technology: one-time ring signature
Currency: VCC(dynamic)
Block speed: 10s
Each sunrise block: 8640
Peak value of TPS: 80,000
Key features: public verifiability, absolute anonymity, high concurrency and high scalability.

DYNAMIC ADJUSTMENT OF TRADING DIFFICULTY

Cryptozoic contains a localization algorithm that changes the difficulty of each block. As the network hash grows or shrinks dramatically, this reduces system response time and keeps blocking probability constant. The original bitcoin method calculates the relationship between the actual and target time span of the last 2016 block and uses it as a coefficient of the current difficulty. It is obviously not suitable for rapid recalculation(because of high inertia) and causes oscillations.

The general idea behind our algorithm is to summarize all the work done by the node into the time

taken. The amount of work is the corresponding difficulty value in each block. However, due to inaccurate and untrusted timestamps, we cannot determine the exact time interval between blocks. The user can move his timestamp to the future, and the next interval may be negative. There are probably very few such events, so we can sort timestamps and truncate outliers (that is, 20%). The remaining values range from 80% of the time taken by the corresponding block.

BLOCK SIZE LIMIT

Users pay for storage blocks and have the right to vote. Each miner handles the balancing of fees and benefits and sets his own "soft limits" to create blocks. In addition, the core rule of maximum block size is necessary to prevent block chains from being flooded with spurious transactions, but the value should not be hard-coded. Let MN be the median of the last N block sizes. So the "limit" for accepting the block size is 2 times MN. It prevents the mass from expanding, but still allows the limit to grow slowly over time if needed. Transaction size does not need to be explicitly limited. It is limited by the size of the block;If someone wants to create a huge transaction with hundreds of inputs/outputs (or a ring signature with a high degree of ambiguity), they can do so by paying enough.

Oversized fined miners still have the ability to fill their own zero-fee transactions up to a maximum of 2•Mb. Although only the majority of miners can adjust the median value, there is still a possibility that the block chain will expand and generate additional loads on the nodes. To prevent malicious participants from creating large chunks, we introduce a penalty function: NewReward = BaseReward•. BIksize0.2mn - apply this rule only if the BIkSize is larger than the minimum available block size (10kb, MN• 110%). When overall fees exceed fines, miners are allowed to create "normal size" blocks, even exceeding profits. But the cost can't be increased twice as much as the penalty, so there's a balance.

MINER CLASSIFICATION

In Ethereum, all transactions including ordinary transfer transaction and smart contract execution are processed and executed by a unified mining machine. Due to different transaction types (transfer transaction and contract execution), different calculations and storage are required, so gaslimit is different. Ethereum USES different gaslimits to force the increase of transaction cost, which is an unscientific approach. Cryptozoic will optimize this, and different transaction types need to be executed by different miners, including:

Transfer & trading miner, contract processing miner.

Transfer & trading miner: handle ordinary VCC transaction.

Transfer & trading miner: deal with smart contract, all kinds of ERC token transactions.

Advantage:

(1) Speed up transactions.

(2) Increase TPS for transactions.

(3) Reduce miners' fees for smart contract processing.

THE ISSUANCE MECHANISM OF VCC

There is no limit on the total issuance of VCC, which is mainly divided into two parts: pre-mining stage and ecological mining stage. VCC produced in pre-mining stage is mainly used for Cryptozoic start-up, reward ecology and TWIN-EX. When the Cryptozic dandelion network is large enough, the Cryptozic will enter a virtuous cycle of autonomy, and VCC issuance will also enter the stage of ecological mining. In the stage of ecological mining, issuance quantity and mining difficulty will be adjusted according to market supply and demand, and the VCC produced by ecological mining will be more widely used.

PREMINING VCC

In the initial stage of the project, a part of VCC will be pre-excavated by Cryptozoic block chain system in an open and transparent way to serve as the initial ecological construction fund of Cryptozoic, so as to ensure the smooth implementation of basic ecological cooperation. Premining contains hidden funds with TWIN-EX VCC.

VCC ECOLOGICAL MINING

After the end of pre-mining, the block chain system will automatically open the ecological mining stage. The Cryptozic mining method is the same as ETH, which only accepts the mine form, not the single mining machine. All the VCC generated by mining will be rewarded to the miners.

Total number of seconds per day: 86,400
Block speed: 10s
Daily block: 8640
Mining is divided into two periods: gold panning period, gold mining period.
During the gold panning period, miners who entered the Cryptozoic at the early stage were encouraged to actively participate in mining activities. The gold rush was rewarded handsomely, as the picture shows.

Block start height	End height of block	Block spacing	Block rewards
1	1,280,000	1,280,000	64
1,280,001	3,840,000	2,560,000	32
3,840,001	7,680,000	3,840,000	16
7,680,001	12,800,000	5,120,000	8
12,800,001	19,200,000	6,400,000	4

Gold mining period: when a large number of miners enter the Cryptozoic to mining, the reward VCC gradually tends to be balanced. Starting from the height of 19,200,001 block, the reward is constant 2 VCC.

Cryptozoic miners use token incentive mode to provide power for miners, and Cryptozoic miners follow POS consensus mechanism. Miners can try to create and validate blocks. Cryptozoic networks are created and validated by thousands of miners around the world at the same time.

Each miner submits a block to the blockchain with a "proof" of the mathematical mechanism. This proof comes from the predefined algorithm of Cryptozoic public chain. The algorithm is difficult, which is also the mechanism of VCC production reduction.

In order for a block to be added to the main chain, a miner must provide this "proof" faster than others. The process of confirming each block by "proof" of a mathematical mechanism provided by the miners is called proof of stake. The miners who obtain the "certificate" broadcast the block to the network, and other miners receive the broadcast to verify the block, and then enter the block chain. In the meantime, the system sends a VCC reward to the miners who produce the block.

CRYPTOZOIC ECOLOGY

FISSION FINANCE ECOLOGY

VCC is a general proof of the value of Cryptozoic ecology. The consensus degree of VCC determines the growth rate and maturity of Cryptozoic ecology, and its value comes from the consensus.The higher the degree of consensus, the greater the value of VCC. If consensus is the root of finance, then fission is the branch of finance. Fission enables rapid growth of consensus of values in a short period of time and promotes ecological development. Cryptozoic's original twin-ex Mining mechanism and dandelion social network have created a sustainable fission environment, on which any fission financial application can be conducted. The dandelion network firmly binds these fission individuals together, making the VCC value network large and stable.

Cryptozoic is not a fixed mode environment and its fission mode can be extended. Future users who use Cryptozoic systems or make secondary development based on Cryptozoic systems can design more novel fission modes based on their own designs. These fission modes will be stored in the system for the whole Cryptozoic ecology to call.

DEVELOPER ECOLOGY

Cryptozoic system will provide a friendly development environment for blockchain enthusiasts and developers around the world. Perfect API, SDK components and basic supporting facilities will help developers quickly integrate into Cryptozoic ecosystem.

Building gateway based on Cryptozoic

Cryptozoic system is a decentralized system that can support high concurrency of financial applications. We do not set restrictions on developers, and developers themselves deploy system gateways to achieve block chain technology and product model compatibility.

Developing application program based on Cryptozoic

Cryptozoic is committed to fully supporting decentralized applications from the technical level, especially through the introduction of mobile terminal strategy, to productize different

DApp ideas, so that ordinary Internet users can truly feel the value brought by blockchain technology.

DApp application oriented to the financial field can bring blockchain technology to more users. For example, financial decentralized financial management, decentralized asset management, decentralized lending, decentralized liquidation, etc. Through the introduction of incentive mechanism, the concept of sharing economy will be further utilized to change the existing APP market and business model.

Block chain technology provides infrastructure to Decentralized Applications. In Cryptozoic system, through the perfect API design, the preparation work of developers can be simplified, so that developers can quickly get started with the corresponding development work. The fission mode within Cryptozoic system will encourage developers to develop high-quality DApp.

Research and development innovation based on Cryptozoic

Cryptozoic developers to make innovations and technical improvements on the basis of Cryptozoic, develop decentralized protocols based on different application scenarios and Cryptozoic, and propose suggestions for improvement of Cryptozoic technology.

PRIVACY ANONYMOUS ECOLOGY

Cryptozoic provides an absolutely anonymous environment for global participants. Anyone containing personal privacy, trade secrets or non-disclosure information can be granted Cryptozoic to conduct transactions.

Hide IP

Cryptozoic uses shield mechanism to hide IP’ s real address, which can effectively reduce attacks. By the usage of two high hardware firewall single-line server as the port to map two IP of double-line server, the virtual IP will be mapped in real IP host, which can avoid being a direct target, and also hide the real IP of double-line server, meanwhile, enhancing the hardware firewall of single-line.In brief, the real IP is hidden, mapping virtual IP to real IP, so as to form absolute defense against DDoS attacks. The processing pf virtual IP mapping does not have permission to log in remotely.

Anonymous account/address

The Cryptozoic uses obfuscating technology to hide the true address of a transaction, so that even if you can trace the amount of each transaction through the blockchain, the actual address is not the real address of the transaction. Cryptozoic makes it impossible to track the real Mining object behind the transaction under verifiable conditions, which is beneficial to protect the security of both parties.

DISTRIBUTED APPLICATION ECOLOGY

DApp is the future development trend. Cryptozoic is not only a huge financial system, but also a stable and reliable DApp operating system. We encourage application developers to use our system to run.

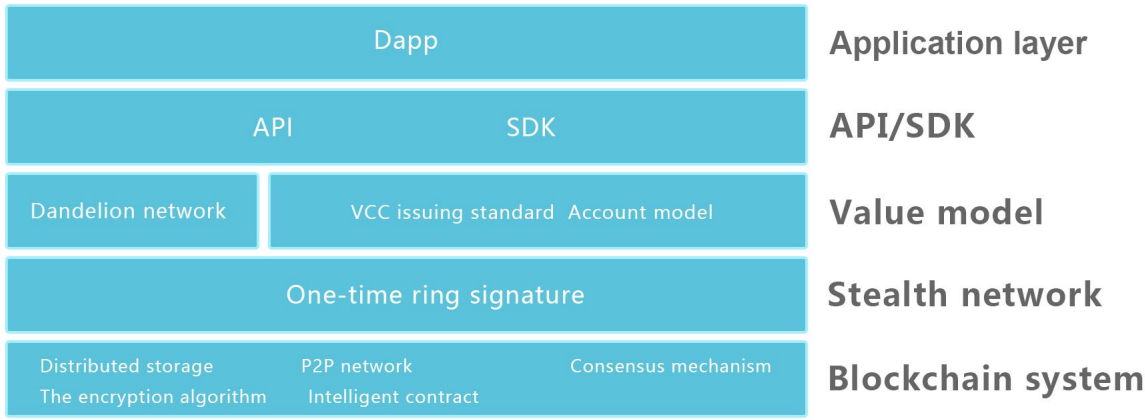
Theoretically, Cryptozoic is a decentralized operating system supporting the development of any financial system. In fact, block chain technology, fission mode and dandelion network based on Cryptozoic can be compatible with any application development. Even if the developer does not have financial attribute in the original intention, they can still develop DApp of corresponding industry based on Cryptozoic , which can not only meet its original demand, but also give more financial attribute.

ASSET MANAGEMENT ECOLOGY

Cryptozoic itself supports multi-chain and multi-currency management and is currently compatible with storage and transfer of VCC, ETH and BTC assets. The Cryptozoic is open to the outside world in terms of asset management, allowing other digital asset developers to open the asset management ecology based on the Cryptozoic. The Cryptozoic itself is an application ecology based on finance, which is beneficial to absorb global digital assets and form a complex digital information management network. Based on this, the hidden universe will also provide financial management, lending and other services around the asset management.

CRYPTOZOIC SYSTEM ARCHITECTURE

Cryptozoic is an open source blockchain application system based on privacy and anonymity technology. Cryptozoic has high concurrency performance and supports commercial applications with average TPS above 8000. The Cryptozoic universe is simply divided into five layers, namely, block chain system, privacy network, value network, API/SDK and application layer, from the bottom up.



BLOCKCHAIN SYSTEM

Distributed storage

Blockchain consists of multiple parties to store data and maintain data security. Many nodes form a distributed network through network communication and consensus mechanism. Blockchain data storage is essentially distributed storage. Data storage is done on multiple network nodes. The only data stored in a single node in distributed network is not recognized. Distributed ledger allows each node to participate in monitoring the legitimacy of the data, but also to jointly prove the data, solving the traditional centralized database monopoly management and security problems. Due to node enough, theoretically, unless an attack on all the nodes in the same time, to block chain tampered with, add or delete the data, however, in fact, nodes are independent existence, and communication has the certain time difference, so the distributed storage is a very safe and trusted storage.

The distributed network storage system adopts the expandable system structure, using several storage servers to share the storage load, using the locationserver to locate the storage information,

it not only improves the safety, availability and storage efficiency of the system, but also is easy to expand.

A standard distributed system without any specific business logic constraints will have the following characteristics:

Distribution

Multiple computers in a distributed system will be randomly distributed in space, and other distribution will change at any time.

Equivalence

There is no master or slave in the distributed system. There is no master or slave that controls the whole system. All the nodes in the distributed system are equal.

Concurrency

In a computer network, the program is running the concurrency in the process of operation is a very common behavior, for example the same distributed multiple nodes of the system, and may concurrently operate some shared resources, such as database or distributed storage, how to accurately and efficiently coordinate distributed concurrent operation has become the one of the biggest challenges in the distributed system architecture and design.

Fault tolerance

All computers that make up a distributed system are subject to failure of any kind. Even if there is a node outage or error, it is necessary to ensure that the distributed system can continue to operate normally, so distributed storage must have a certain degree of fault tolerance.

Peer-to-peer (P2P) network

Peer-to-peer (P2P) technology, also known as "peer-to-peer" or "Peer" technology, relies on the computing power and bandwidth of each node in the network, rather than clustering in several central servers. Before the P2P technology, all web applications using C/S or B/S structure to achieve, but in C/S architecture before application, the client request to the server software, server and then respond to client requests, in this case, if the client, the more the greater the pressure on the server at this time. However, each computer implemented by P2P technology is

both a client and a server, and their functions are equivalent. Data transmission and communication can be carried out directly between nodes in the network.

BLOCKCHAIN SYSTEM

Decentralization

Resources and services in the network are scattered on all nodes, and the transmission of information and the realization of services are carried out directly between nodes, which can avoid the intervention of intermediate links and servers and avoid possible bottlenecks. The basic characteristics of P2P decentralization bring its advantages in scalability and other aspects.

Scalability

In P2P network, with the addition of users, not only the demand for services increases, but also the overall resources and service capacity of the system expand synchronously, which can always meet the needs of users easily. In theory the scalability is almost infinite.

Resistance to attack

P2P architecture inherently has the advantages of attack resistance and high fault tolerance. Because the service is distributed among the nodes, some nodes or network damage has little impact on other parts.

P2P networks can automatically adjust the overall topology and maintain the connectivity of other nodes when some nodes fail.P2P networks are usually set up in a self-organizing way, allowing nodes to freely join and leave.

High cost performance

Performance advantage is an important reason why P2P is widely concerned. With the development of hardware technology, the computing and storage capacity and network bandwidth of personal computer are increasing rapidly according to Moore's theorem. P2P architecture can effectively utilize a large number of common nodes distributed in the Internet to distribute computing tasks or storage data to all nodes. Make use of the

the idle computing power or storage space to achieve the purpose of high performance computing and mass storage.

Privacy protection

In P2P network, the possibility of eavesdropping and leakage of users' privacy information is greatly reduced because the transmission of information is distributed among nodes without going through a centralized link. In addition, at present, the technology of relay forwarding is mainly used to solve the Internet privacy problem, thus hiding the participants in the communication in many network entities.

In some traditional anonymous communication systems, the implementation of this mechanism depends on some relay server nodes. In P2P, all participants can provide relay forwarding function, which greatly improves the flexibility and reliability of anonymous communication and provides better privacy protection for users.

Load balancing

In the P2P network environment, each node is both a server and a client, which reduces the requirement on the computing power and storage capacity of the traditional C/S structure server. At the same time, because the resources are distributed in multiple nodes, the load balance of the whole network is better realized.

CONSENSUS MECHANISM

In the Cryptozoic , we propose and study a new working verification algorithm. Our main goal is to close the gap between CPU (majority) and GPU/FPGA/ASIC (minority) miners. It is appropriate that some users may have certain advantages over others, but their investment should grow linearly with the growth of electricity. More broadly, the production of specialized equipment must be as profitable as possible.

Related work

The original ETH work protocol used the CPU-intensive pricing feature sha-256. It is mainly composed of basic logical operators and only depends on the computation speed of the processor, so it is fully applicable to multi-core/transmitter implementation. However, modern computers are not limited by the number of operations per second, nor by the size

of memory; Although some processors can be much faster than others, the memory size is unlikely to change from machine to machine. The memory pricing function was defined as the function that "computing time is dominated by the time spent accessing memory". The main idea is to build an algorithm that allocates large amounts of data in memory (" registers ") that can be accessed relatively slowly (such as RAM) and "access unpredictable sequences of locations". A block should be large enough to have an advantage over recalculating per access. The algorithm should also prevent internal parallelism, so N concurrent threads should need N times of memory at a time. Dwork investigates and formalizes this approach, leading them to propose another variation of the pricing function: "Mbound". Another task belongs to F. Coelho, who proposed the most effective solution: "Hokkaido"; the last algorithm based on the idea of pseudo-random search in large arrays is called "scrypt". Unlike previous features, it focuses on key derivation rather than work proof system. Despite this fact, scrypt can serve our purpose: it has a good pricing feature in the partially dispersed column conversion problem, such as SHA-256 in Bitcoin. Currently, scrypt has been applied to Litecoin and other bitcoins. However, its implementation is not really memory bound: the ratio "memory access time/total time" is not large enough because each instance uses only 128 KB. This makes GPU miners about 10 times more efficient, and leaves open the possibility of creating relatively cheap but efficient mining equipment. In addition, the scrypt construct itself allows for a linear tradeoff between memory size and CPU speed, due to the fact that each block in the register comes from only the previous block. For example, you could store every other block and recalculate the other blocks lazily, that is, only when it becomes necessary. Pseudo-random index is assumed to be uniformly distributed, so the expected value of additional block recalculation is 1•N, where N is the number of iterations. Overall computation time increased by less than half, because there are time independent (constant time) operations, such as preparing the buffer and hashing to save 2/3 of the memory cost per iteration 1•N + 1•2•N = N additional recalculations. 3, 3, 9/10 is 1 times N plus...+ 1, 9, N = 4.5 N. It is easy to show that only one 10 of all blocks is stored for 10 seconds with an increase of less than s-1 factor. This in turn means that a machine with a CPU is 200 times faster than a modern chip and can store only 320 bytes of memory.

Proposed algorithm

We propose a new memory limitation algorithm for work pricing. It relies on random access to slow memory and emphasizes delayed dependency. Compared to each new block (64 bytes in length), it depends on all previous blocks. So a hypothetical "memory protection" should increase its computational speed exponentially. Our algorithm requires approximately 2 Mb per instance for the following reasons: it is suitable for modern processors' L3 cache (per core). A Megabyte of internal memory is an almost unacceptable size for modern ASIC pipes. GPUs may run hundreds of concurrent instances, but are

limited in other ways: GDDR5 memory is slower than CPU L3 cache, and its bandwidth is significant, rather than random access speed. The significant expansion of the register will require an increase in the number of iterations which in turn means an increase in the overall time. Heavy calls in untrusted p2p networks can lead to serious vulnerabilities, as nodes are obliged to check the work certificates of each new block. If a node spends a significant amount of time in each hash evaluation, it can easily DDoS with a large number of dummy objects with arbitrary working data (random values).

Encryption algorithm

Cryptozoic adopts two excellent encryption algorithms based on hash algorithm, which are applied in block validation, mining difficulty, privacy and anonymity, etc.

Sha256

RSA public key encryption algorithm was developed by Ron Rivest, Adi Shamirh and LenAdleman in 1977. RSA takes its name from the development of all three of them. RSA is the most influential public key encryption algorithm, which can resist all known password attacks so far, and has been recommended by ISO as the public key data encryption standard. RSA's algorithm is based on a very simple number theory fact: it is easy to multiply two large prime Numbers, but it is extremely difficult to factor the product, so the product can be exposed as an encryption key.

RSA algorithm is an asymmetric cryptography algorithm. The so-called asymmetric algorithm means that the algorithm needs a pair of keys, and if one of them is used to encrypt, the other one is needed to decrypt, which is widely used in blockchain. Asymmetric encryption in the application of the blockchain mainly has two aspects, one is to prove the role, the second is to encrypt the content.

Digital signature means that the sender, issuer or owner of the data will use the private key to encrypt the data. Other holders of the public key can verify whether the data has been tampered or whether it is issued by the private key holder himself by using the corresponding public key of the encrypted data. The UTXO transaction of digital certificate is signed by asymmetric encryption algorithm. The public key is used as the account address, and the private key is used as the digital signature for each transaction of the account, so as to determine the flow direction of assets.

SHA256 is the main cryptographic hash function used to construct blockchain. This hash function is used to calculate the hash value of the relevant data, whether it is the header information of the block or the transaction data, so as to ensure the integrity of the data. For example, in the bitcoin system, a consensus mechanism for workload proof is designed based on finding the SHA256 hash value of a given prefix. SHA256 is also used to construct digital pass-through addresses to identify different accounts.

SHA256 is an iterative hash function with Merkle-Damgard structure. Its calculation process is divided into two stages: message preprocessing and main loop. In the preprocessing stage of the message, it mainly completes the filling and extended filling of the message, converts the original input message into n 512-bit message blocks, and then uses the SHA256 compression function to process each block. This calculation process is an iterative calculation process. When the last message block (the Nth block) is processed, the final output value is the SHA256 value of the original message input.

（2）Elliptic curve algorithm

Elliptic curve group is composed of two parts:

The first part is M.There are two numbers a and b in region F

M = y^2 = x^3 + ax + b where x,y belong to F*F

The second part is O point (infinity point)

(group of elliptic curves)E = O U M

After knowing the definition of elliptic curve group, the images on the coordinate axis must be different according to the different parameters.

For the convenience of research, elliptic curves about the X-axis can be stacked:

y^2 = x^3 - x.The image represented is an elliptic curve on the left and a semi-open shape similar to the less than sign on the right.

Addition on elliptic curves (geometric representation)

The selection of two points on the curve can be divided into the following three situations:

1. When the two points selected are not identical (the two points selected here are generally similar to those on the ellipse). And the line between the two points is not parallel to the Y-axis.So the elongated line segment must intersect another point on the curve, which is P, and the intersection point P, which is parallel to the Y-axis, intersects another point on the ellipse P', which is the result of adding these two points.

2. If the same points are selected, the tangent line of this point on the ellipse will intersect at a point again (the remaining steps are the same as 1.).

3. If the extension line connected to two points is parallel to the Y-axis, the sum of the two

points will be O at infinity.

Addition on elliptic curves (mathematical description)
(1) P + O = O + P = P.
(2) P=(x1,y1),Q =(x2,y2) is a member of E.
1.O if x1 is equal to x2 and y1 is equal to minus y2
P plus Q is equal to 2.(x3,y3) something else
Where / x3 = t^2-x1-x2/1.(y2-y1)/(x2-x1) if P!=Q (dot plus operation)
Point R = \ y3 = t (x1 - x3) - y1, and t = \ 2. (3 * x1 ^ 2 + a)/(2 y1) if P = Q (multiply operation)
So x3,y3 has three outcomes.
So what we're trying to prove is why do we have these three outcomes?

A. Discuss and prove the value of t
P=(x1,y1) ,Q = (x2,y2), which is a member of E
1. When P != Q, the slope at both points is t = (y2-y1)/(x2-x1).
2. When P = Q, the derivative at P (Q) is t = dy/dx
Take the derivative of both sides of the equation y^2 = x^3 + ax + b, and you get:
2y*(dy/dx) = 3x^2 + a
And t = (dy/dx) = (3*x1^2+a) / (2y1).

B. Prove the third intersection of line y = tx + c and elliptic curve y^2 = x^3 + ax + B
So we can combine the above two equations to get an equation of t and x, which is:
x^3-t^2*x+(a+2tc)*x+b-c^2 = 0
Let R'=(x3,-y3) be the third point outside of pq.
So x1+x2+x3 = t^2.
You can evaluate x3 here, and then you can substitute into the equation of the line and you get y3 , and you get y3 minus and you get y3.

Smart contracts

Smart contracts are an idea put forward by Nick saab in the 1990s, almost the same age as the Internet. Because of lack of trusted execution environment, smart contract has not been applied to the actual industry, since after the birth of the currency, people realized that the underlying technology of the currency block chain natural can provide smart contracts with trusted execution environment, the etheric lane first saw chain blocks and smart contract correspondence, issued a whitepaper " Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform", and has been committed to the Ethernet lane into the

best intelligence platform, so the currency lead block chain while ethereum revive smart contracts.

Simply put, smart contract is the digital version of the real contract, which is to program the real contract parties and their responsibilities and obligations in the computer. Certain conditions and rules are set in the smart contract, which can make the contract run automatically without manual operation and execute the agreed content of the contract. Without a reliable operating environment, it is not safe for smart contracts to run naked on the Internet. Such contracts can be maliciously attacked by people, but blockchain can provide a reliable operating environment. An smart contract is a computer program running on a blockchain database that can execute itself when it meets the conditions written in its source code. Once the smart contract is written, it can be trusted by users. Blockchain guarantees that the terms of the contract cannot be changed once it is linked up.

Smart contracts can be used for trading and any exchange between two or more parties. The code contains conditions that trigger automatic execution of the contract. Once coded, the smart contracts are uploaded to the blockchain network, where they are sent to all devices connected to the network. Once the data is uploaded to all devices, users can agree on the results of executing program code. The database is then updated to record the performance of contracts and to monitor the terms of contracts to check compliance. The smart contract itself is also a system participant. It responds to the information it receives. It can receive and store value. It can also send information and value out.

A complete smart contract must have the following elements:

Contract participants

Participants of smart contract can be both parties or multiple parties. The information and attribution division of participants will be written into the code of smart contract. Once the participants of smart contract running in the block chain environment are written, they cannot be changed and must take their own role.

Contents of the execution of the contract

The execution content of smart contract is mainly the rights and obligations of both parties. In the transaction smart contract, it is the number and mode of transaction.

Timing of contract execution

The smart contract is in a dormant state when it is not executed. It will only be triggered when sufficient conditions are met, which may be time limit or certain quantity limit.

Judge whether the execution is done or not

smart contract needs to determine whether the event that has met certain conditions has been executed, and whether the execution is successful or not, so as to facilitate the feedback of the performance of smart contract to developers.

NETWORK OF PRIVACY

Cryptozoic uses a one-time circular signature to make the sender completely anonymous in the way of sending privacy transactions. The protocol based on one-time ring signature allows users to realize unconditional connectionless. Common types of encrypted signatures allow for tracking of their respective sender and receiver transactions. The key to address this deficiency is the different signature type used in current electronic cash systems. Firstly provide a general description of algorithm without explicitly mentioning e-cash. One-time ring signature consists of four algorithms: (GEN, SIG, VER, LNK): GEN: take public parameters and output ec pair (P, x) and public key i. SIG: obtain message m, public key Sr Pi, I f = s, a pair (Ps, xs), and output signature sigma and a set of s = Sr union {Ps}. VER: canceling message m, collection S, signature sigma, and printing "true" or "false". LNK: take the set I = {Ii}, sign sigma and output "link" or "independence". The idea behind the protocol is fairly simple: a user generates a signature that can be checked by a set of public keys rather than a single public key. The identity of the signer and the user whose public key is in it are indistinguishable until the owner USES the same keyword to generate the second signature.

GEN: the signer selects the random key x∈[1, 1-1], and calculates the corresponding public key P = XTT. In addition, he calculates another public key I = xHp (P), which we call the "key image". SIG: the signer uses the technology to generate a one-time ring signature with non-interactive zero-knowledge proof. He selected Sr, a random subset of n, from other users' public key Pi, his own key pair (x, P), and the key image I. Let 0≤s≤n be the secret index of the signer in s (making his public key Ps). He picks a random {qi | I = 0...N} and {wi | I = 0...N, i*f* = s} from （1。。I），applies the following transformation: Ii = Ri =.qitt, if i = s qitt + wiPi, if if = s If i = s qiHp (Pi) + wiI, then if if = s next step is to get non-interactive

challenge: c = Hs (m, L1,..., Ln, R1..., Rn) finally, the signer computes the response: wi, if f = s ci =n ri = c -. ci mod l, if i= s i = 0, if f = s qs-csx mod l, if i= s, the signature is σ= (I, c1, ..., cn, r1, ..., rn) . VER: the verifier checks the signature by applying inverter: i= ritt + ciPi Ri = riHp (Pi) + cil N + finally, the verifier checks whether. ci = Hs (m, Lr, ..., Lr, Rr, ..., Rr) mod l I = 0 0 N 0 N if this equality is correct, the verifier runs the algorithm LNK. Otherwise, the verifier refuses to sign. LNK: the verifier checks to see if I have been used in past signatures (these values are stored in set I). Multiple uses mean that two signatures are generated under the same key. Protocol meaning: by applying the L transform, the signer proves that he knows that x has at least one Pi = XTT. In order to make this proof unrepeatable, we introduce the key image as I = xHp (P). The signer USES the same coefficient (ri, ci) to prove almost the same statement: he knows such x, at least one Hp (Pi) = I•x-1. If the mapping x→I is an injection: no one can recover the public key from the key image and identify the signer; the signer cannot sign two signatures with different me and the same x.

Security

We will give proof of our one-time signature scheme. In a way, the proof is partially consistent and rewritten with references, rather than forcing it from paper to paper.

These are the attributes to build: Linkability. For all secret keys of a given set S {xi} I = 1, it is not possible to obtain n + 1 active signatures ofσ1, σ2。 。 。 , σn+ 1, and the LNK phase is obtained for all of them (i.e., with n+ 1 different key images Ij). This attribute implies double expenditure protection in the context of CryptoNote. Ability to explain. For a given set of S, an image of xi (excluding I = j) with a maximum of n-1 corresponding private keys, and an image of key xj, Ij cannot produce a valid signature σ of an Ij. This attribute implies theft protection in the context of CryptoNote. Non-forgery. Given only one public key set S, it is impossible to obtain a valid signature sigma.Anonymity. Given a signature sigma and corresponding set S, it is not possible to determine the signer's secret index j with probability p> 1.

Connectivity

Theorem 1. Our one-time ring signature scheme is chaining of random oracle model -- certification: assuming that an opponent can represent any i, j∈[1] generates n + 1 valid signature with a key imageσiii*f* = Ij。 。 。 N]. Due to #S = n, at least one Ii f = xiHp (Pi) for each i. Consider the corresponding signatureσ= (I, c1,..., cn, r1..., rn). VER (σ) = "true", meaning Lr i = ritt + ciPi ☒Rr☒ i = riHp (Pi) + cil ñ . ci = Hs (m, Lr, ..., Lr, Rr, ..., Rr)

mod l | l = 1 1 N 1Ñ the first two equality means a generation i.logG Lr = ri + cixi log HP（PI） Rr = ri + ci log Hp（Pi）I where logA B informally represents the discrete logarithm from B to base A. We note that $I: xi = logHp (Pi) I means that all ci's are unique. The third time equality forces the opponent to find the previous image of Hs to successfully attack the event whose probability is considered negligible.

Theorem 2. Our one-time ring signature scheme can be ignored under the assumption of discrete logarithm in the random oracle model. Certificate. Suppose the opponent is able to produce a valid signature σ=（I，c1，...，cn，r1，...，rn），where I = xj HP（Pj）given {xi | i = 1，。。，j-1，j + 1，...。。，n}. Then, we can construct an algorithm A to solve the discrete logarithm problem in E (Fq). Suppose that inst = (tt, P) ∈ E (Fq) is a given instance of DLP, and the goal is to obtain s, such that P = stt. Using standard techniques, A simulates the random and signature words and enables the opponent to produce two active signatures of σ=（I，c1，...，cn，r1，...，rn）和σr=（I，cr，...，cr，rr，...，rr）.1 n 1 n rj-rt is due to I = xj Hp (Pj) in the two signatures, we calculate xj = logHp (Pj) I = ct moda A output xj, because Lj = RJTT + cj Pj = rr tt + cr Pj and Pj = P.

Security

We will give proof of our one-time signature scheme. In a way, it is consistent with the parts proved in [24], but we decided to rewrite them with references, rather than forcing the reader to go from paper to paper.

These are the attributes to build: Linkability. For all secret keys of a given set S {xi} I = 1, it is not possible to obtain n + 1 active signatures ofσ1，σ2。。。，σn+ 1, and the LNK phase is obtained for all of them (i.e., with n+ 1 different key images Ii). This attribute implies double expenditure protection in the context of CryptoNote. Ability to explain. For a given set of S, an image of xi (excluding I = j) with a maximum of n-1 corresponding private keys, and an image of key xj, Ij cannot produce a valid signature σ of an Ij. This attribute implies theft protection in the context of CryptoNote. Non-forgery. Given only one public key set S, it is impossible to obtain a valid signature sigma.Anonymity. Given a signature sigma and corresponding set S, it is not possible to determine the signer's secret index j with probability p> 1.

Non-forgery

Non-forgery is only one meaning of linkability and excludability;

Theorem 3. If the one-time ring signature scheme is linkable and can be cancelled, it is not forgery -- certification: suppose the opponent can forge the signature of a given set S: σ0= （I0，...）. Consider all valid signatures (defined as honest signatures) for the same message m and set S: σ1，σ2，。。。，σn. There are two possible scenarios: I0∈{Ii n. Which ones are illegal.I0 ƒ ∈ {Ii n. Which contradicts linkability.

Anonymous

Theorem 4. Our one-off ring signature scheme is anonymous under the deterministic Diffie-hellman hypothesis in the random oracle model.
Certification: suppose the opponent can determine the signer's secret index j with probability p = 1 + s. Then, we can construct algorithm A, which solves the decisive diffie-hellman problem in E (Fq) with the probability of 1 + s.2. Set inst = (tt1, tt2, Q1, Q2) ∈E (Fq) as an instance of DDH, and determine whether logG1 Q1 = logG2 Q2.

σ0= （I，...） provides to the opponent, where Pj = xjtt1 = Q1 and I = Q2, simulate oracle Hp, return tt2 to query Hp (Pj). Opponent returns k as his guess on index i: I = xiHP (Pi). If k = j, A returns 1 (for "yes"), otherwise A random r∈{1,0}. The probability of correct selection is: 1 + Pr (1 | inst∈DDH) -Pr (1 | inst∈DDH) = 1 + Pr (k row = j | inst∈DDH) + 2 2 Pr (k row = j | inst∈/ DDH) -Pr (k row = j | inst∈/ DDH) -Pr (k row = j | inst∈/ DDH) -Pr (k row = j | inst∈/ DDH) -Pr (k row = j | inst∈/ DDH) = 1, 1, 1, 1, 1, 1, 1, 1, s 2 + n + s + (n-s) • 2-n -N •2 = 2 + 2, in fact, the result should be reduced by the probability of collision in Hs, but this value is considered negligible. Notes on Hp, the hash function.

Hp is defined as deterministic hash function E (Fq) →E (Fq). There is no proof that Hp is an ideal cryptographic hash function. The main purpose is to obtain the pseudo-random number of the image key I = xHp (XTT) in a certain way. Using a fixed base (I = xtt2), it may have the following situation: Alice sent to Bob two standard Mining, producing one-off tx key: P2 = the Hs (r1A) tt + B and P1 = the Hs (r2A tt + B) Bob restore corresponds to a private tx key x1 and x2, and spending with a valid signature and image key I1 = x1tt2 and I2 = x2tt2 output. Now Alice can link the signatures and check the equation I1-I2 = (Hs (r1A) -hs (r2A)) tt2. The problem is that Alice knows the linear correlation between public key P1 and P2, and in the case of fixed base tt2, she also obtains the same relationship between key images I1 and I2. Replacing tt2 with HP (xtt2), which does not retain linearity, fixes the defect.

THE VALUE NETWORK

VCC release standard

In order to ensure the normal block release of Cryptozoic block chain system, VCC issued on the basis of Chuangshi block is used as block release incentive. That is to say, for each block produced by miners and provided with effective proof of calculation force, a certain amount of VCC is obtained as reward. The amount of VCC reward will be adjusted according to the difficulty of mining.

The miner packages the transaction into blocks and broadcasts it to the network, finds a random number target, and performs SHA256 calculation on the block head. The calculation results must meet the following requirements:

hash (nonce) = < target
target: the target of difficulty set by the system
target is a variable that will be adjusted after a certain block height.
The miner uses hash algorithm to calculate the given nonce string of the system for many times, and finally calculates the value that meets the condition, that is, the block right is obtained through competition.
hash(nonce) =< target

Every 10s, the miners continue to receive the transaction order (at the same time will do verification), put their reward, the latest block hash value together, calculate the new hash value, see whether to meet the difficulty target, once met, it will produce a new block, and broadcast out. If not, and the new block is received, which means that the round of accounting right competition fails, then reset the process until the calculation is successful.

After the miner successfully generates the block, the system will automatically send a VCC to the miner's account.

account model

Cryptozoic uses UTXO account model.

Each UTXO transaction has a number of transaction inputs, that is, the source of funds, and also a number of transaction outputs, that is, the whereabouts of funds. Each transaction costs an input and produces an output, and the resulting output is "unspent transaction

output," or UTXO. An analogy for a transaction in the UTXO model is a paper bill, where each account keeps track of how much it has by accumulating the number of bills in the account. When we want to spend money, using one or more existing UTXO (bills) is enough to cover costs, and may receive some new UTXO (bills). Each bill can only be used once, because once used up, UTXO is removed from the pool.

The benefits of the UTXO model are:

Scalability: because you can process multiple UTXO's simultaneously, you can implement parallel transactions and encourage scalability innovation.

Privacy: UTXO provides a higher level of privacy. If privacy needs to be enhanced, consider more complex solutions, such as one-time ring signatures.

We'll talk more about dandelion networks and value patterns in parts 6 and 7.

API/SDK

Cryptozoic system will provide developers with compatible API interfaces and SDK toolkits to develop DApps that meet various business requirements. For traditional applications, the transformation from traditional Apps to DApps can also be completed through data interaction.

THE APPLICATION LAYER

Cryptozoic allows other developers to develop multiple ecological applications based on the integrity of the system itself, and encourages developers to make innovative designs based on this. Cryptozoic will be a decentralized application system facing the world with no threshold.

VCC FISSION MODE

The VCC fission mode is inspired by the law of energy conservation.

Financial value is the same as sound, light, heat and other energy principles in nature. The value of VCC comes from the expansion of consensus, while the value of VCC may decline along with the loss of consensus. In order to eliminate this phenomenon, adopt the twin-ex Mining method to ensure the self-regulation of the value of VCC along with the dynamic consensus. TWIN-EX consists of two parts: E2V and V2E.

E2V(one-way trade)

E2V is divided into three stages: IEEX stage, CEEX stage and LEEX stage.

The IEEX only exists in the Cryptozoic dark epoch. Once the project is started, the IEEX will be started.Automatically switch to CEEX (EtherExchangeeX) after IEEX ends. This is the normal phase of E2V, the perpetual currency exchange phase, where the "x "is infinite. According to the natural changes of the market, participants can continuously convert ETH into VCC to obtain more wealth.

Users who participate in E2V transactions must be ETH users. Of course, you can also choose to buy ETH in the market to participate.

The IEEX is divided into four levels, each with 50 steps. Every 200 ETH goes directly into the upper layer.

The initial proportion of the transaction is 1ETH: 1800VCC, and the proportion decreases by 2 VCC layer by layer. Ratio refers to that when you invest a certain amount of ETH, the system will convert the VCC corresponding to the ratio to you. For example, under the premise of the initial conversion ratio of 1ETH: 1800VCC, if you invest 1ETH into the Cryptozoic, the system will return 1800VCC to you. In addition to the VCC obtained, the system will reward VCC by a certain multiple according to your participation in the stage, the first multiple is 5; the second multiple is 4;the three-step multiple is 3; the four-step multiple is 2.

If you are a first-gear participant and you invest in 1ETH, you will receive an additional 5 times *1800VCC in addition to 1800VCC. This is an incentive for users to actively participate in E2V. The earlier they participate, the higher degree of consensus on Cryptozoic will be, so the more

VCC they will obtain.

The formula for calculating the number of VCC obtained per exchange is: the number of VCC obtained per exchange =ETH number *E2V ratio * reward multiple.

After the end of IEEX, it automatically enters the CEEX stage.

It would be simpler for CEEX to have only one step, 700 steps in all, with 200 ETH on each step going directly up the ladder.

The initial exchange rate is 1ETH: 1400VCC, and the ratio decreases by 2 VCC layer by layer. The CEEX award is 1 times.

After the end of CEEX, it automatically enters the LEEX stage.

LEEX has only one step, 100 steps in all, and 200 ETH on each step go directly to the upper step.

The exchange rate is initially 1ETH: 1VCC, which decreases by 0.01 VCC layer by layer. LEEX's reward multiple is still one.

Note: the above formula for calculating the number of VCC obtained each time is: number of ETH *E2V conversion ratio * multiple. If the number of ETH invested is between the upper and lower levels, it will be split and different exchange rates will be calculated respectively.

V2E(repurchase destruction)

Cryptozoic uses a decentralized recovery mechanism called V2E.

VCC repurchase and destruction have been realized. The ETH generated from each transaction will be automatically transferred to the total V2E pool, and the user will voluntarily contribute to the VCC regular settlement, which will be returned to the user ETH. When entering the epoch of expansion (block reaches a certain height), it can trigger to turn on V2E. Participants invest in VCC and convert it into ETH in proportion, which changes dynamically. As the VCC input from users increases, the conversion rate of ETH will decrease. The system automatically issues ETH address to the ETH address of the user participating in the V2E phase.

The user participation condition is: hold 100,000VCC.

ETH number of each period = total number of pools in the previous period (block height reference epoch) *30%. The smaller the number of VCC participating in V2E, the higher the conversion ratio and the larger the number of ETH.

Settlement: the number of ETH obtained by the user in this period is fully convertible according to the ratio of total VCC and total ETH in the destruction pool in this period.

Note: the user can repeatedly invest in the VCC to participate in the destruction mechanism of V2E phase to obtain ETH.

DANDELION NETWORK

The nature of interpersonal relationship –connection.

According to the modern sociological theory of Marx, social communication refers to the mutual contact, communication and exchange between people and other groups in production and other social activities. Social communication helps to improve the productivity of individuals and groups, promote the creation and development of social productivity, and is also a necessary condition for the generation and deepening of social consensus, as well as one of the prerequisites for the realization of communism.

In modern real life, people can become acquainted with each other, which is a way for individuals to establish their own social communication system. The same goes for connecting individuals to a group. By establishing connections with others or groups, individuals can expand their communication scope and power, thus forming a huge social communication system that is beneficial to them.

Individuals know hundreds or thousands of people directly, or indirectly, through people they know directly. Others in a person's social network also establish social networking relationships with others directly or indirectly. The network structure of direct, indirect and mutual knowledge is abstracted into a graph, which is not a tree structure or even a line structure, but a three-dimensional and closely connected network structure like dandelion.

In Cryptozoic anonymous network system, Cryptozoic establishes a social relationship network architecture similar to dandelion -- dandelion network structure. This is a truly decentralized, free, anonymous relational network structure.

In this structure, everyone on the network is a point, each point has a direct relationship with the point directly adjacent. And for each of these neighboring points, there are other points that are directly related to these neighboring points.Points establish a relationship with adjacent points, and even can establish an adjacent relationship with other points that are not adjacent, forming a closer and more direct connection. This is just like the human network in real life. When a new point is generated, it connects the social relation network of adjacent points, and can be extended infinitely through these adjacent points, and the adjacent points can also be extended infinitely through the relation network of this point.

In the dandelion network structure, each point is connected to form a tight whole. This network has no center, because every point is the center. It has no boundaries. It can connect and extend indefinitely.

Everyone is the center, not the center, that is decentralization.

When each person enters the dandelion network, a unique identification ID, namely CAID, will be generated after the anonymous identity authentication verification of Cryptozoic public chain. So, everyone is anonymous, just a digital ID, I am me while you are you. Everyone is a sources in the dandelion network, waiting to be discovered and discovered, or from this point, to establish proximity to other points.

Dandelion network is different from the hiepochrchical relationship in the traditional financial model.

Hierarchy relation is a kind of multi-center relation network. The so-called multi-center is to spread with multiple source points. Source points are the core individuals of the network, and the core individuals fission through their own relation network.Subordinates of these source points can only form a link relationship with their superiors or subordinates. Once the relationship is formed, they can no longer establish a relationship with other individuals. If they do not comply, this will be regarded as betrayal by the network. Hierarchical relation network is a multi-center network centered on the source point. The power of discourse and decision-making of the whole network lies in the source point, and all the subordinates of the source point can only follow.

Each individual of the dandelion network can establish adjacent relationships at will, which will not be restricted by anyone. The dandelion network gives Cryptozoic fully decentralized consensus relationships.

CAID

To access the Cryptozoic network, a Cryptozoic Anonymous Network Identity belonging to individuals needs to be created: CAID(Cryptozoic Anonymous Identity), which we shall refer to as CAID for short. CAID is the capacity identification in Cryptozoic network. It is like the premise and key that users use to unlock and add various functions and applications, such as dandelion network and flying program. Entering the Cryptozoic, you will receive a basic account identity and activate CAID in two ways.

Direct activation: obtain the user CAID who has joined the Cryptozoic anonymous network, and pay 50 VCC to establish an adjacent relationship with this user. After successful establishment, the unique anonymous CAID can be generated.

Exploration activation: if it is impossible to find CAID that has joined Cryptozoic network, through the unique flying program of dandelion network, randomly explore a CAID that enables flying program to establish a proximity relationship, that is, if it succeeds, 50 VCC will be paid.

VCC paid by CAID will be distributed to CAID users(namely target recluse), rangers fund, recluse fund and other CAID in adjacent path in a certain proportion, and partially destroyed by creating Cryptozoic anonymous identity through the above methods.

After CAID is created successfully, it establishes an adjacent relationship with adjacent points. In the dandelion network, it is particularly important to establish an individual social communication system. The larger the individual's social interaction system, the greater and wider the rewards that come with. Usually, a CAID can increase the number of adjacent points by inviting others to activate directly, but it cannot establish the closest proximity relationship with existing CAID in dandelion network, or even CAID which has a large number of adjacent points. At this time, through the dandelion flying program and exploration program to achieve this purpose, to maximize the impact of the network.

PATH REWARDS FOR CAID

CAID path rewards are designed to encourage CAID fission and reinforce dandelion networks by building proximity relationships.The reward comes from the VCC paid by the newly activated CAID. Specific rewards are as follows:

The VCC of establishing adjacent payment is divided into three parts, namely, sharing revenue (80%) and fund contribution (10%), and smart contract automatic destruction (10%).

60% of the Shared revenue will reward target recluse directly (activate CAID directly to help activate new CAID).

25% of the Shared revenue is divided equally by CAID with the recluse path of "1".

15% of the Shared revenue is divided equally by CAID with the recluse path of "2".

As shown in the figure, target recluse D is taken as an example. If recluse F activates F through CAID of D, its relationship with D is path 1. If F activates VCC paid by CAID, D will get 60% of network sharing revenue, B, G and E will get 25%, and A and C will get 15%.

So we can conclude that the earlier you join the dandelion network, the more rewards you get, the earlier you build proximity, the more rewards you get.

De-duplication mechanism: assume that in the whole network relationship, the character relationship of path 1 and path 2 overlap, and only calculate the income of the current relationship path 1.

FLYING PROGRAM

Flying means the dandelion seeds, with the wind fluttering up> Finally, choose fertile soil to take root and growth into a new dandelion.

In the dandelion network, CAID can actively join the fluttering plan and expose its CAID to the dandelion network. With the endless fluttering of the network, it is waiting to be activated and establish an adjacent relationship with the CAID of the explorer (exploration plan). Once the proximity relationship is established, the social interaction system benefits from other CAID can be Shared.

Enable the fluttering scheme:

(1)It was discovered by explorers, establishing proximity relationships and obtaining benefits from CAID creation;

(2) Obtain the exploration benefits and enjoy the rich benefits brought by the social communication system of both sides, and the exploration benefits will be shared to the adjacent points in a certain proportion.

(3) To start the fluttering plan, 3600 VCC locks are required.

EXPLORATION PROGRAM

Exploration program and flying plan are complementary to each other. Through exploration plan, CAID can find the CAID that started fluttering plan in dandelion network and establish a close relationship with it, so as to expand the scope of CAID's social communication system and obtain more benefits.

(1) Each time we explore, we will randomly select a CAID from the CAID enabled with fluttering plan in the dandelion network to establish an adjacent relationship with the current CAID.

(2) Each exploration needs to pay 50 VCC. The paid VCC will be distributed proportionally to the starters of the fluttering program, the homeless fund, the recluse fund, the node service fee, etc.

(3) There is no limit to the number of explorations. Each payment of VCC can complete one exploration.

HOMELESS PROGRAM

In China, there is a famous science fiction writer in the world -- Mr. Liu Cixin, who has won the highest achievement award of science fiction in the world. Mr. Liu has written a book, "wandering earth," about an epic plan to escape the solar system to a new home.In honor of this, the Cryptozoic introduced the rangers program.

The flying program and the exploration program are important components of the dandelion network. Through these two ways, CAID's social communication system can be gradually strengthened. In this context, the Cryptozoic network established and enabled the rangers program (rangers fund), a reward system that rewards outstanding contributors and lucky CAID in the current epoch through a variety of leaderboards, random selections, etc.

MOTIVATIONS NETWORKS

The future development of Cryptozoic ecology needs the participation and selfless contribution of most community volunteers, among which there are some excellent ones. In order to encourage more people to participate in the construction of Cryptozoic ecology, we designed a series of incentive methods, which formed the Cryptozoic incentive network.

HERMIT FUND

Since Cryptozoic is born, elite block chain community representatives have the opportunity to join a decentralized free social consensus, building community and groups for Cryptozoic, and ongoing maintenance and promotion. It is a long-term hard work, and hermit fund purpose is as a reward for participants who lead the future development of Cryptozoic communities. Cryptozoic hopes to vote for the elites leading the future development of Cryptozoic ecology through decentralized voting by loyal CAID members. These elites wage war on behalf of the entire Cryptozoic ecology, realizing its autonomy, ensuring efficiency and involving every recluse in development decisions. In this way, everyone is the owner of the Cryptozoic and realizes the important transformation of decentralized democratic ecology.

Hermit fund comes from the payment expenditure, capture activation CAID and exploration plan established by CAID, a dandelion network.

In each epoch, when the Cryptozoic public chain reaches a certain block height, the system will judge which hermit provides the most autonomous services according to the consensus of the whole network, and put it into the alternative list. Each epoch has a list of 10080(number of blocks), the greater the contribution, the greater the chance of being selected to the list.

Note: the more hermit with path 1, the more services to community construction, the higher the probability of being an alternative.

When it reaches the height of the last block of each epoch, the system automatically opens the voting channel, and each CAID has only one voting opportunity. Those who participate in the voting need to lock up 100 VCC to get the voting opportunity. After locking up the storehouse, the system cannot automatically open the storehouse. Voting recluses need to send VCC special transactions

to the candidates they want to support. The system will update the election results when the block reaches the next epoch. The VCC automatically unlocks voters' positions.

The rewards for hermit funds are divided into two parts: one part is a reward for voters, and those who participate in the voting (those who support are authorized to become elite hermits) can share 40% of the recluse funds equally; 60 percent of the recluse funds will be distributed equally to 20 elite recluses and those whose periphepochl paths are 1 or 2.

IMPLICIT FAMILY FUNDS

In the first stage, the project has just been launched. Part of the premining VCC will be used as the initial ecological construction fund of Cryptozoic in an open and transparent way to ensure the smooth implementation of basic ecological cooperation.

The initial ecological construction fund is 50,000,000VCC, which is mainly allocated to special contributors and consensus communities, such as community construction, media platform cooperation, data platform cooperation, exchange cooperation and mining pool cooperation bonuses.

NODE REWARD

Super node

Before the height of the block was 1,280,000, only 128 users were allowed to participate. The current lockup of 126,000 VCC could obtain 30% of the newly produced VCC. Settlement by block day.

Make a wish program

All users can participate. Lock 1000 VCC at current time, and get 5% of the newly produced VCC from mining, which is settled by block daily.

REWARDS FOR BELIEVERS

Lucky believers

Qualification of believers: must be active CAID and participate in the VCC lockers of 9900.

Lucky believers win the bid: from the believers who meet the requirements, each TWIN—EX 50ETH will produce one winning quota, with no limitation.

Reward ETH: 20%ETH from the E2V pool of the last microera. The winners will be divided into 60 percent, 25 percent for those who follow the path of 1 hermit and 15 percent for those who follow the path of 2 hermit.

Super believers

Qualification as a believer: must be an activated CAID with 48,000 VCC locks.

Super believers win the bid: only 200 users before the height of block 128000.

Reward ETH: split 20%ETH in the E2V pool of the previous micro epoch, according to the daily settlement of blocks. Those who believe in the prize are equally divided into 60%, 25% for those who follow the path of 1 recluse and 15% for those who follow the path of 2 recluse.

E2V MINING LEADERBOARD

Statistical rules: reach a certain height of the last block of each micro-epoch, count the number of each address participating in E2V, rank top20 in order from most to least, and participate in the calculation of rewards.

Invisible targets with paths of 1 and 2 will be radiated with rewards, 60% of invisible targets, 25% of paths of 1 and 15% of paths of 2, and rewards for TOP20 invisible targets will be distributed in the form of "arithmetic difference".

ROADMAP

With the continuous exploration and evolution of Cryptozoic network, more and more users will join the anonymous and free Cryptozoic dandelion network. In the dandelion network, individuals have limited influence in social communication, which leads to limited benefits in the network. Only by constantly expanding the influence, exert the power of the network and groups, get more benefits.

CAID's continuous improvement of personal social communication influence also brings strength and influence to the huge social communication system of dandelion network. Therefore, Cryptozoic rewards these outstanding contributions through a phased model of impact creation.

The epoch, according to the development stage of Cryptozoic ecology, is divided into dark epoch, topological epoch, expansion epoch and constant epoch. Among them, each epoch in the development process, also divided into a number of micro epoch. When the Cryptozoic chain blocks reach a certain height, it will end the current epoch (or micro epoch) and enter the next epoch (or micro epoch). When the epoch ends, in the Cryptozoic network according to the established rules, from the rangers fund,hermit fund expenditure will be rewarded to excellent users.

Dark epoch

The dark epoch (genesis) is the first epoch of Cryptozoic . During this epoch, E2V Mining mechanism will be automatically enabled, V2E destruction mechanism will be shut down, and dandelion fluttering plan, exploration plan, rangers fund and recluse fund will be available. (see section E2V for more "IEEX mechanism")

The dark epoch is divided into four microages, which are archean, ancient, proterozoic and Mesozoic. The last Mesozoic epoch ended with the height of the block reaching a certain point and entered the epoch of topological.

Topological epoch

During the topological epoch, every 60480 blocks was a microepoch, with a total of 12 microepoch. After the end of the 12th microepoch, it entered the third epoch - expansion epoch.

During the topological epoch, E2V Mining mechanism will automatically end, V2E destruction mechanism will automatically open,dandelion flying plan, exploration program, rangers fund, hermit fund available.

Expansion epoch

The first application of XXEX (anonymous exchange) Mining on the Cryptozoic public chain, VCC value is determined by the market.

Constant epoch

Constant epoch belongs to the conservation of wealth phase, will be committed to the chain of ecological development and application.

UNORGANIZED OPERATION

Cryptozoic hopes to create an anonymous blockchain ecology without centralization. Based on the free consensus society of all participants, Cryptozoic is not owned by individuals or organizations, and the ecosystem is forged by developers and participants. The progress of Cryptozoic project depends on the participation of community members. We will grade the contributions of community members and give them different rewards.

WARM TIPS

LEGAL NOTICES

This is a conceptual whitepaper to explain in detail the concepts and core technologies of Cryptozoic underlying operating system (hereinafter referred to as "Cryptozoic") and Cryptozoic Token (hereinafter referred to as "VCC"). This document is subject to constant revision, but Cryptozoic is under no obligation to update this white paper on a regular basis or to provide any additional information. Please read the following in detail:

Not open to everyone:

Cryptozoic and VCC are not open to everyone. Anyone who wants to participate needs to complete a series of steps and provide specific information and documentation.

No controlled products are available in the jurisdiction:

This whitepaper does not constitute a prospectus or offer of any kind nor is it intended to constitute an offer or offer for any securities or any regulated product in any jurisdiction. This whitepaper has not been reviewed by regulatory authorities in any jurisdiction.

No suggestions:

This whitepaper does not constitute a recommendation as to whether you should participate in the Cryptozoic universe or purchase VCC, nor should it be the basis for your decision to do so.

Without any representations or warranties:

We do not guarantee the accuracy and completeness of the information, statements, opinions or other matters in the white paper. Without limitation, we make no representations or warranties as to the achievement or reasonableness of any forward-looking or conceptual statement. Nothing in the white paper shall be used as a basis for any future commitment or statement. We are not liable for any loss caused by the white paper.

The English version shall prevail:

This whitepaper is available in English only. Any translation is for reference only and is not authenticated by any person. If there is any discrepancy between the translation of this white paper and the English version, the English version shall prevail.

You must listen to all necessary and professional financial and legal advice: including communicating and dealing with relevant matters with tax, accounting and lawyers, and being reminded by these professionals that digital assets and platforms involve risks. You must assess the degree of risks and your affordability. As the laws related to blockchain and digital assets are becoming more and more mature, please pay attention to the update of laws related to your host country and your nationality.

RISK WARNING

As a new investment mode, digital asset investment has various risks. Potential investors need to carefully evaluate investment risks and their tolerance of risks:

Marketing risk

As the VCC sales market environment is closely related to the overall situation of the digital money market, such as the overall market downturn, or the existence of other uncontrollable factors, it may cause the price of VCC itself, even if it has a good prospect, is still in a long-term state of undervaluation.

Competitive risk

With the development of information technology and mobile Internet, digital assets represented by "bitcoin" are gradually emerging, various decentralized applications continue to emerge, and competition in the industry is increasingly fierce. However, with the endless emergence and expansion of other application platforms, the community will face continuous operational pressure and certain market competition risks.

Lack of capital leads to the risk of failure to develop

Due to the substantial decline in the price of digital assets raised by the founding team or the exceeding of the development time, the team may suffer from a lack of development

funds, which may lead to the extreme shortage of funds and the risk that the original development goal cannot be achieved.

Risk of loss of private key

After the VCC of the purchaser extracts its own digital wallet address, the only way to operate the contents contained in the address is the relevant key of the purchaser (i.e. private key or wallet password). It is the individual responsibility of the user to protect the relevant key used to sign a transaction certifying ownership of the asset.The user understands and accepts that if his private key file or password is lost or stolen respectively, the VCC obtained related to the user's account (address) or password will not be recoverable and will be permanently lost. The best way to store login credentials securely is for the purchaser to store the keys securely in one or more places, preferably not on a public computer.

The risk of uninsured loss

Unlike bank accounts or other financial institutions, where there is usually no insurance on Cryptozoic accounts or related blockchain networks, there will be no published individual organization to cover your losses in any case.

Systemic risk

The risk of overlooked fatal flaws in open source software or massive failures of global network infrastructure. While some of these risks will be significantly reduced over time, such as fixing vulnerabilities and breaking computing bottlenecks, others remain unpredictable, such as political factors or natural disasters that could disrupt some or all of the world's Internet.

Vulnerability risk or the risk of accelerated development of cryptography

The accelerated development of cryptography or technology, such as quantum computers, may bring the risk of cracking Cryptozoic , which may lead to the loss of VCC. Although this stage is not developed theoretically, it is not ruled out.

Application failure risk

Cryptic eon may fail due to various known or unknown reasons (such as large-scale node

outage) and cannot provide normal service, which may lead to the loss of user VCC.

The risk that the application or product fails to meet the expectation of itself or the purchaser.

Cryptic eon related application is currently under development, before issuing an official version could make a big change, any VCC buyer about hidden raw main application or its functionality or form (including the participants' behavior expectations or imagination could not meet expectations, any error analysis, a design change, etc are likely to lead to the happening of this kind of situation.

REFERENCES

[1] http://bitcoin.org.

[2] https://en.bitcoin.it/wiki/Category:Mixing Services.

[3] http://blog.ezyang.com/2012/07/secure-multiparty-bitcoin-anonymization.

[4] https://bitcointalk.org/index.php?topic=279249.0.

[5] http://msrvideo.vo.msecnd.net/rmcvideos/192058/dl/192058.pdf.

[6] https://github.com/bitcoin/bips/blob/master/bip-0034.mediawiki#Specification.

[7]https://github.com/bitcoin/bips/blob/master/bip-0016.mediawiki#Backwards Compatibility.

[8] https://en.bitcoin.it/wiki/Mining hardware comparison.、

[9] https://github.com/bitcoin/bips/blob/master/bip-0050.mediawiki.

[10] http://luke.dashjr.org/programs/bitcoin/files/charts/branches.html.

[11] https://bitcointalk.org/index.php?topic=196259.0.

[12] https://en.bitcoin.it/wiki/Contracts.

[13] https://en.bitcoin.it/wiki/Script.

[14] http://litecoin.org.

[15] Mart´ın Abadi, Michael Burrows, and Ted Wobber. Moderately hard, memory-bound func- tions. In NDSS, 2003.

[16] Ben Adida, Susan Hohenberger, and Ronald L. Rivest. Ad-hoc-groupsignatures from hi-jacked keypairs. In in DIMACS Workshop on Theft in E-Commerce, 2005.

[17] Man Ho Au, Sherman S. M. Chow, Willy Susilo, and Patrick P. Tsang. Short linkable ring signatures revisited. In EuroPKI, pages 101–115, 2006.

[18] Daniel J. Bernstein, Niels Duif, Tanja Lange, Peter Schwabe, and Bo-Yin Yang. High-speed high-security signatures. J. Cryptographic Engineering, 2(2):77–89, 2012.

[19] David Chaum and Eug`ene van Heyst. Group signatures. In EUROCRYPT, pages 257–265, 1991.

[20] Fabien Coelho. Exponential memory-bound functions for proof of work protocols. IACR Cryptology ePrint Archive, 2005:356, 2005.

[21] Ronald Cramer, Ivan Damg˚ard, and Berry Schoenmakers. Proofs of partial knowledge and simplified design of witness hiding protocols. In CRYPTO, pages 174–187, 1994.

[22] Cynthia Dwork, Andrew Goldberg, and Moni Naor. On memory-bound functions for fighting spam. In CRYPTO, pages 426–444, 2003.

[23] Eiichiro Fujisaki. Sub-linear size traceable ring signatures without random oracles. In CT- RSA, pages 393–415, 2011.

[24] Eiichiro Fujisaki and Koutarou Suzuki. Traceable ring signature. In Public Key Cryptography, pages 181–200, 2007.

[25] Jezz Garzik. Peer review of "quantitative analysis of the full bitcoin transaction graph". https://gist.github.com/3901921, 2012.

[26] Joseph K. Liu, Victor K. Wei, and Duncan S. Wong. Linkable spontaneous anonymous group signature for ad hoc groups (extended abstract). In ACISP, pages 325–335, 2004.

[27] Joseph K. Liu and Duncan S. Wong. Linkable ring signatures: Security models and new schemes. In ICCSA (2), pages 614–623, 2005.

[28] Ian Miers, Christina Garman, Matthew Green, and Aviel D. Rubin. Zerocoin: Anonymous distributed e-cash from bitcoin. In IEEE Symposium on Security and Privacy, pages 397– 411, 2013.

[29] Micha Ober, Stefan Katzenbeisser, and Kay Hamacher. Structure and anonymity of the bitcoin transaction graph. Future internet, 5(2):237–250, 2013.

[30] Tatsuaki Okamoto and Kazuo Ohta. Universal electronic cash. In CRYPTO, pages 324–337, 1991.

[31] Marc Santamaria Ortega. The bitcoin transaction graph — anonymity. Master' s thesis, Universitat Oberta de Catalunya, June 2013.

[32] Colin Percival. Stronger key derivation via sequential memory-hard functions. Presented at BSDCan' 09, May 2009.

[33] Fergal Reid and Martin Harrigan. An analysis of anonymity in the bitcoin system. CoRR, abs/1107.4524, 2011.

[34] Ronald L. Rivest, Adi Shamir, and Yael Tauman. How to leak a secret. In ASIACRYPT, pages 552–565, 2001.

[35] Dorit Ron and Adi Shamir. Quantitative analysis of the full bitcoin transaction graph. IACR Cryptology ePrint Archive, 2012:584, 2012.

[36] Meni Rosenfeld. Analysis of hashrate-based double-spending. 2012.

[37] Maciej Ulas. Rational points on certain hyperelliptic curves over finite fields. Bulletin of the Polish Academy of Sciences. Mathematics, 55(2):97–104, 2007.

[38] Qianhong Wu, Willy Susilo, Yi Mu, and Fangguo Zhang. Ad hoc group signatures. In IWSEC, pages 120–135, 2006