PROJECT X

WHITE PAPER

A new business ecosystem based on
gemel-blockchain technology

CONTENTS

01
ABSTARCT

On November 1, 2008, the concept of blockchain was first proposed by Nakamoto Satoshi. Bitcoin was officially born on January 3, 2009. It has been 10 years since then. In the past 10 years, countless people have been convinced by the genius design of Nakamoto. Being attracted by the myth of Bitcoin's creation, they entered the world of blockchain. With the continuous exploration of blockchain technology, people gradually find that blockchain can be applied in various fields of human activities. More and more people are beginning to believe that blockchain will be an indispensable technology in the future world. It even has the potential to become an underlying system similar to the Internet.

However, we have to admit that the current blockchain technology is not mature, especially the existing "impossible triangle". It means that the blockchain technology cannot simultaneously decentralize, security and efficiency. Any blockchain project can only meet two goals at the same time, so people still tend to choose traditional solutions when solving practical problems.

If the problem of "impossible triangle" cannot be solved, the application scenario of blockchain technology will be very limited, so that it will not be able to form a universal solution, neither to say becoming a bottom system of human society. In order to solve this problem, we must return to the underlying logic of the problem and think about the formation of the "impossible triangle."

We believe that the basic problem is that all current projects are subjected to the design of Bitcoin. The basic setting of designing only one chain is the most important problem for blockchain technology. The efficiency of blockchain technology is one problem that has been mostly criticized. And the reason is that "one" itself represents limitation, so that it cannot express thousands of changes in the real world.

Inspired by the double-helix structure of DNA molecules, we creatively combines bionics with blockchain technology to design a blockchain project with a double-stranded structure: Project X. The two chains of Project X are developed with different technologies, carrying part of the information of the other part. Compared with one chain, it is more stable, and the security is geometrically multiplied. With the help of a series of interactive technologies, different concepts can be integrated and packaged to be compatible and complement to each other.

Our goal is to create a blockchain system that offers endless possibilities and build bridges between different ideas. Blockchain technology will be redefined, and a new generation of public chain standards is expected to be born.

02
PROJECT INTRODUCTION

2.1 PROJECT CONCEPTS

2.2 X GEMEL-BLOCKCHAIN TECHNOLOGY IS THE LIGHT OF HOPE TO SOLVE THE IMPOSSIBLE TRIANGLE OF BLOCKCHAIN

2.3 THE FAR-REACHING SIGNIFICANCE OF THE BLOCKCHAIN FUTURE

2.1 PROJECT CONCEPTS

The core of the Project X is the double-stranded structure. The idea comes from bionics. In the actual design process, we get inspiration from the double-stranded structure of DNA. We believe that the double stranded structure can overcome the blockchain “impossible triangle” problem.

In order to solve the "impossible triangle" problem, we review the history of blockchain technology development to find out the cause of the problem.

In the early days, Bitcoin was mainly used for illegal transactions, which generally led the central governments to a contradiction against Bitcoin. The voices of questioning and opposing Bitcoin also appeared. In order to create "better bitcoin", people began to reflect and try to change some of Bitcoin's attributes and developed some new projects. For example, in order to reduce energy consumption, some projects abandoned the Proof Of Work (POW) and adopted the Proof Of Stake (POS); some projects adopted a relatively centralized design to improve transfer efficiency; others also use technical means to enhance anonymity, thus achieving extreme freedom and decentralized goals, etc.

At this stage, people continue to try and choose, summing up the famous blockchain "impossible triangle" law: any blockchain project can only meet two goals at the same time among decentralization, security, efficiency.

Pursuing "safety" and "decentralization" requires sacrificing “efficiency”. The original intention of Bitcoin is the combination of “decentralization” and “security.” Every node in the network stores all the data, which brings high storage and verification costs, resulting in inefficiency. Only 7 transactions can be processed in seconds within Bitcoin network, which cannot carry large-scale payment needs.

Pursuing "efficiency" and "decentralization" requires sacrifi-cing “security”. Ethereum added smart contract functionality to Bitcoin. Since then, a large number of projects have been developed based on Ethereum, and all transactions have been conducted on the Ethereum network, which has improved efficiency compared to Bitcoin. However, the smart contract code on the Ethereum blockchain is all public, which means that all vulnerabilities are public. The more powerful the smart contract, the more logically complex and the more vulnerable the code. The safety of Ethereum has always been the problem everyone should pay attention to.

PROJECT INTRODUCTION

Pursuing "efficiency" and "security" requires sacrificing "decentralization". Due to the increasing number of transfers, Bitcoin's own block capacity has become a bottleneck. In the process of improving this problem, there has been a divergence between the miners and the development team in the community. The miner's block expansion plan has improved the performance requirements of the nodes. The idea is to reduce the degree of "decentralization" in order to ensure "efficiency" and "security." however, the development team's lightning network solution uses branch nodes to calculate small amount of frequent transactions and integrates them into the main chain at regular intervals. This solution can reduce the write pressure of the main chain, which is equivalent to increasing the capacity of the main chain. Since this scheme requires the use of specialized branch nodes, it actually reduces the degree of “decentralization."

After the establishment of the "impossible triangle" law of the blockchain system, in order to meet different needs, the development ideas of the new project mostly seek a balance point in "decentralization", "security" and "efficiency". For example, the design idea of the EOS project is to use the DPOS mechanism to sacrifice a part of “decentralization” and pursue “efficiency”, that is, higher transaction throughput, on the basis of ensuring “security”. Similarly, under the “impossible triangle”, all projects face a basic problem: how to choose the balance point? Which one of the “decentralization”, “security” and “efficiency” have the highest priority?

The answer to this question can be found in Maslow's hierarchy of needs. Maslow divides human needs into five categories from low to high: physical needs, security needs, social needs, respected needs, and self-fulfilling needs. When mapping "impossible triangles" to human needs, security represents the highest priority; the efficiency of blockchain system mainly refers to the number of transactions processed per second, and the transaction behavior involves human-to-human interaction, and corresponds to social needs to some extent, making efficiency the second priority; and decentralization corresponds to human respected needs and self-fulfilling needs, and its relative priority is the lowest because decentralization expresses the public's desire for equality. This is also the reason why EOS projects choose safety as first priority, efficiency second, and decentralization third.

PROJECT INTRODUCTION

EOS has made reasonable choices under the "impossible triangle”. But in the reality, the safety and efficiency of EOS is still unsatisfactory. In fact, the actual application of most of the current blockchain projects is still in the theory, and can not bring substantial changes to human activities. If the existing blockchain projects can't break the "impossible triangle" mindset, the application scenarios of blockchain technology will be greatly limited, and many practical problems will continue to seek solutions in the traditional field. Some people have hoped that the solution of the problem will be tackled by upgrading hardware, but the comprehensive performance of the traditional solution will increase after the hardware upgrade as well, so the gap will become larger and larger. The majority of the ways to solve problems within the existing technical framework may be on the wrong path, because we have observed that the majority of developers only study and improve blockchain technology from the perspective of technology itself. Each technical solution to the problem will bring new problems. In the long run, blockchain technology will increasingly deviate from the original purpose.

After reviewing the reasons for the formation of the "impossible triangle" problem of blockchain, in order to find a solution to the problem, we broke the mindset and rethought the underlying logic of blockchain technology. We constantly tried to stand out of the blockchain technology to look at the problem, and finally get important inspiration from the natural world.

Since ancient times, nature has been the source of all kinds of human technical ideas, engineering principles and major inventions, especially the various creatures in nature. After several billion years of natural selection, the best solutions survived. In recent decades, people have recognized that biological systems are one of the main ways to open up new technologies, and began to use the biological world as a source of various technical ideas, design principles and inventions.

The core function of blockchain technology is to record information, and the biosphere has provided us with one of the best templates - DNA. As the genetic material of most organisms, the most important function of DNA is to carry genetic information, which is consistent with the core functions of blockchain technology. Every cell in the organism has its own genetic information, which is consistent with the decentralization of blockchain technology.

The specific expression of DNA genetic information is a combination of four different base arrangements. The information sequence carried on two single strands of DNA is different, but the two strands can be complementary after binding, which makes the structure of DNA molecules stable to guarantee the safety of information. Most of the changes in genetic information are harmful and unhelpful.

PROJECT INTRODUCTION

The single-strand mutation requires only one base change, and the double-strand is changed simultaneously by a pair of bases. Therefore, the DNA double-strand structure can greatly reduce the probability of mutation. Inspired by bionics, with reference to the double-stranded structure of DNA, we found that all blockchain projects that encounter the bottleneck of “impossible triangle” default to one premise: there is only one chain in the blockchain project. One chain means limitation. Once a contradiction or a dilemma is encountered, a trade-off must be made. Most developers default to the single-chain structure of blockchain technology, and exclude the possibility of two chains from the beginning.

After jumping out of the mindset, we will not be subject to any restrictions on the existing blockchain technology regardless of “impossible triangle” or decentralization. We will develop a double-stranded project “Project X” as compared to find a balance point in the chain of the existing projects. From a broader perspective, we are not only solving the problem of “impossible triangle”. Project X has higher goals and pursuits.

Project X is not just a subversive innovation at the technical level. Our goal is to reunite consensus, seek common ground while reserving differences among different ideas, and guide people to refocus their attention on technological progress itself, and establish a communication channel between different groups of human society.

When looking back at the ideological background of the birth of Bitcoin, we can see that the global economy generally declined after the outbreak of the subprime mortgage crisis in 2009. Many people were disappointed with the central bank-led legal currency system, and then questioned the centralized government, leading to the emergence of the anarchist trend of thought.

The total amount of bitcoin created by Nakamoto has a limited ceiling, which is in sharp contrast to the central bank’s indiscriminate currency. The decentralized mining method is also in line with the liberals, and that’s why Bitcoin became the ideal currency form of among liberals and anarchism in the early years. They believe that Bitcoin can become the global currency, bringing the ultimate freedom to the world. However, on the other hand, due to the extremely difficult supervision, the initial application scenarios of Bitcoin are mainly illegal activities such as smuggling and money laundering. This has caused central banks to suppress Bitcoin. The mainstream media of the government-led media reports on Bitcoin are mostly negative. Traditional financial communities also hold a resistance attitude towards Bitcoin, arguing that Bitcoin has no value.

On the surface of this divergence, there are ideological differences. We can temporarily call this the contradiction between freedom and autocracy, and the root cause is interest. Most of the early supporters of Bitcoin is away from the center of the world's political and economic power, and they naturally do not agree with the government's taxation and inflation caused by the issuing of more currency. Those who oppose Bitcoin rely more on the redistribution of wealth by central organizations such as the government and financial institutions, and Bitcoin has somehow weakened their control and economic interests.

But as time goes by, Bitcoin supporters have gradually found that Bitcoin has become more and more centralized as well. A small number of people controlled most of the Bitcoin. The computing power is also concentrated in several large mining pools. The development trend is not the same as the decentralization that people expected, and many people have tried to introspect. Centralized organizations represented by governments and financial institutions have gradually accepted Bitcoin and invested resources to tap the potential of blockchain technology. An iconic event is that Bitcoin futures have also entered the formal exchange, which means that Bitcoin has become a generally accepted commodity.

The reason is that the core idea of the so-called "decentralization" of the blockchain is not certain. One of the classifications of blockchains is the public chain, the alliance chain, and the private chain. The private chain has become a completely centralized technology. Since the fully centralized chain also belongs to the blockchain, it can be seen that the idea of decentralization is not the label of blockchain technology. In fact, the concept of decentralization never appeared in Nakamoto's Bitcoin white paper. Decentralization may be just a symbolic meaning that early supporters gave to bitcoin. As a technology, centralization or decentralization is not fixed.

The controversy of Bitcoin is slowly diminishing, but we believe that Bitcoin is only a tool for opposing ideas. Maybe Bitcoin and blockchain technology will be recognized by most people in the future, but people who advocate freedom will find another tool to fight against power. Different ideas will continue to create conflicts in other areas. Both sides are striving for the maximization of their own interests, but the resulting contradictions and conflicts have always affected the overall interests of human civilization. Without the channels of communication, the two sides will fall into a prisoner's dilemma, making it difficult to reach deeper cooperation. This is a key issue that restricts the development of human civilization.

Whether it is freedom or autocracy, it will bring serious problems once it goes to extremes. This lesson has been taught too many times in human history, but so far human beings have been swaying back and forth between the two extremes, trying to find the ultimate solution. In the early stage, Bitcoin moved to the extreme of freedom and bring short-lived consensus to the people who advocate freedom, but over time, the alienation appears among the people who advocate freedom. Some people also intentionally or unintentionally become the vested interest group after gaining wealth and voice. Their mind changed accordingly, thus moving to the other extreme. From the continuous division of the Bitcoin community, it can be shown that Bitcoin can't really bring the consensus of all mankind, so that the possibility of becoming the world currency in the future is very small.

Project X combines two chains representing different ideas, symbolizing the integration of two seemingly contradictory ideas of freedom and autocracy, and provides a channel for mutual transformation. Different ideas will begin to communicate and produce mutual trust in Project X. The best way to solve the prisoner's dilemma is to communicate, and one of the functions of the blockchain itself is to generate machine trust. We believe that with Project X as the bridge, human beings can finally gather a common consensus, which is our ultimate goal.

We believe that Project X will become the representative of the new generation of public chain to point out a new path for the development of blockchain technology and build a bridge for the consensus among different groups of human beings.

2.2 X GEMEL-BLOCKCHAIN TECHNOLOGY IS THE LIGHT OF HOPE TO SOLVE THE IMPOSSIBLE TRIANGLE OF BLOCKCHAIN

Taking a look at the current mainstream blockchain projects with the largest market value and influence, Bitcoin and Litecoin have good decentralization and security, but their scalability is poor, and the overall performance can not meet the commercial needs. Meanwhile, the POW mining method wastes a lot of energy. Ethereum has better decentralization and scalability, but the more complex the system, the more vulnerable the leaks. It was forced to diverge in respond to the DAO hacking incident. Its security and performance is still not good enough to support applications with large traffic. Although Ripple's performance is strong and its security is relatively high, it is essentially a product of centralization. EOS is more balanced and scalable. Although some of the decentralized attributes are sacrificed to improve performance, the performance of EOS is not as expected. If the super nodes choose to do evil, its security is also doubtful.

PROJECT INTRODUCTION

Project X jumped out of the mindset of one chain, using complementary symbiotic double-stranded structures to solve the problem of "impossible triangle." Similar to most projects, we must put security issues in the first place.

One of the core functions of the blockchain system is to greatly increase the cost of distorting information, thus ensuring the security of the information. This is consistent with the function of DNA to ensure that genetic information cannot be easily changed. Like DNA, we believe that the double-stranded structure has a natural advantage in security issues. In the specific design and implementation process, part of the information in each chain of Project X will be stored in another chain at the same time. If the attacker try to tamper with the information on the chain, he has to attack both chains simultaneously. However, the two chains adopt different algorithms and operating mechanisms, so that the difficulty of the attack increases geometrically.

With the double-stranded structure to enhance the overall security of the system, we have more room to design the two chains with high efficiency and high level of decentralization.

Consider Both Efficiency And Decentralization

Consensus Algorithm

A new consensus algorithm based on DPOS algorithm - XPOS algorithm

Avoid Bifurcation

Use Directed Acyclic Graph (DAG) to avoid bifurcation

Decentralization

The method of secretly and randomly selecting the temporary member nodes allows the pursuit of efficiency while taking into account the centralization.

Promote Anonymity And Freedom

Consensus Agorithm

Consensus mechanism is random POW

Mining Mechanism

Disperse mining using the Equihash algorithm

Privacy Protection

Uses simple non-interactive zero-knowledge proof mechanism to guarantee anonymity and privacy protection, and designs a cross-chain fragmentation consensus algorithm to take into account efficiency.

PROJECT INTRODUCTION

The two chains of Project X are called the white X chain and the black X chain, respectively. They are both using the most advanced blockchain technology. The white X chain focuses on high efficiency, where the consensus mechanism XPOS (an improved version of the DPOS consensus mechanism) is adopted.

The possibility of bifurcation is reduced by the directed acyclic graph (DAG) organization block, and the temporary member nodes are selected secretly and randomly to ensure decentralization. The black X chain represents extreme freedom and anonymity, where the random POW consensus mechanism is adopted. The Equihash algorithm is used to spread mining, and the simple non-interactive zero-knowledge proof mechanism is used to guarantee anonymity and privacy protection. Also, the cross-chain fragmentation consensus algorithm is designed to balance efficiency.

The two differently focused chains form a symbiotic system through the control of the double-stranded cross-link protocol we developed, allowing the Project X project to meet multiple distinct needs at the same time. Taking into account the scalability, security and decentralization, the X double-stranded system overcomes the impossibility triangle of blockchain.

Let’s view back to the impossible triangle of the blockchain. The X double-stranded randomly selects the temporary member nodes and the black X chain uses the Equihash algorithm to spread the mining to ensure that the entire network can be decentralized to the greatest extent.

Meanwhile, relies on the white X chain node member system (including a chairman node with detached power) and the black X chain cross-chain fragmentation consensus algorithm, the workload of the X double-stranded chain is greatly reduced. This also improves efficiency and ensures network scalability.

The temporary member nodes in the white X chain verifier are randomly and secretly selected. Even if they are corrupted in an instant, they can't tamper with or withdraw the news they send out. The cost of standing member nodes playing tricks are extremely high. They have absolute power to respond quickly so that the security is extremely guaranteed. In addition, the use of DAG to organize blocks also minimizes the possibility of bifurcation. The black X chain uses a simple non-interactive zero-knowledge proof mechanism, so that the computing tasks themselves can be verified without being executed. In this case, the security and anonymity are guaranteed to the greatest extent.

2.3 THE FAR-REACHING SIGNIFICANCE OF THE BLOCKCHAIN FUTURE

Since the birth of the first blockchain project that mimics Bitcoin, most developers have only tried to improve on the basis of Bitcoin, but few people are thinking about how to make subversive innovations. The 2.0 version of the blockchain represented by Ethereum has greatly reduced the difficulty of project development in the form of an open source blockchain platform. But from another perspective, this approach also limits the creativity of developers on existing platforms. The projects developed based on the existing platform are not innovative when it comes to technology.

Under the limitation of “impossible triangle”, the existing blockchain technology can't surpass the traditional and centralized solution in most application scenarios. We are inspired by the DNA double-strand structure and creatively propose a double-stranded model of the blockchain, which is expected to completely solve the "impossible triangle" problem.

We hope that the mindset of philosophy and bionics will allow all developers to rethink the nature of blockchain technology, and look for cross-border integration of blockchain technology in various fields.

The purpose of Project X is not only to solve the "impossible triangle" problem of blockchain technology. We believe that Project X will redefine the blockchain project. In the future, Project X will become an underlying system of human activities, and become the DNA of blockchain projects, Internet projects, and even the human civilization, to continuously promote the evolution of human civilization and pass on the glorious achievements of human civilization.

03
TECHNICAL ARCHITECTURE

3.1 TWO DIFFERENT CONSENSUS MECHANISMS

3.2 SELECT NODES USING VERIFIABLE RANDOM FUNCTION VRF

3.3 USING ZKSNARK TO ENSURE STRONG ANONYMITY

3.4 ORGANIZE BLOCKS WITH DIRECTED ACYCLIC GRAPHS TO AVOID BIFURCATION

3.5 CROSS-CHAIN TECHNOLOGY

3.1 TWO DIFFERENT CONSENSUS MECHANISMS

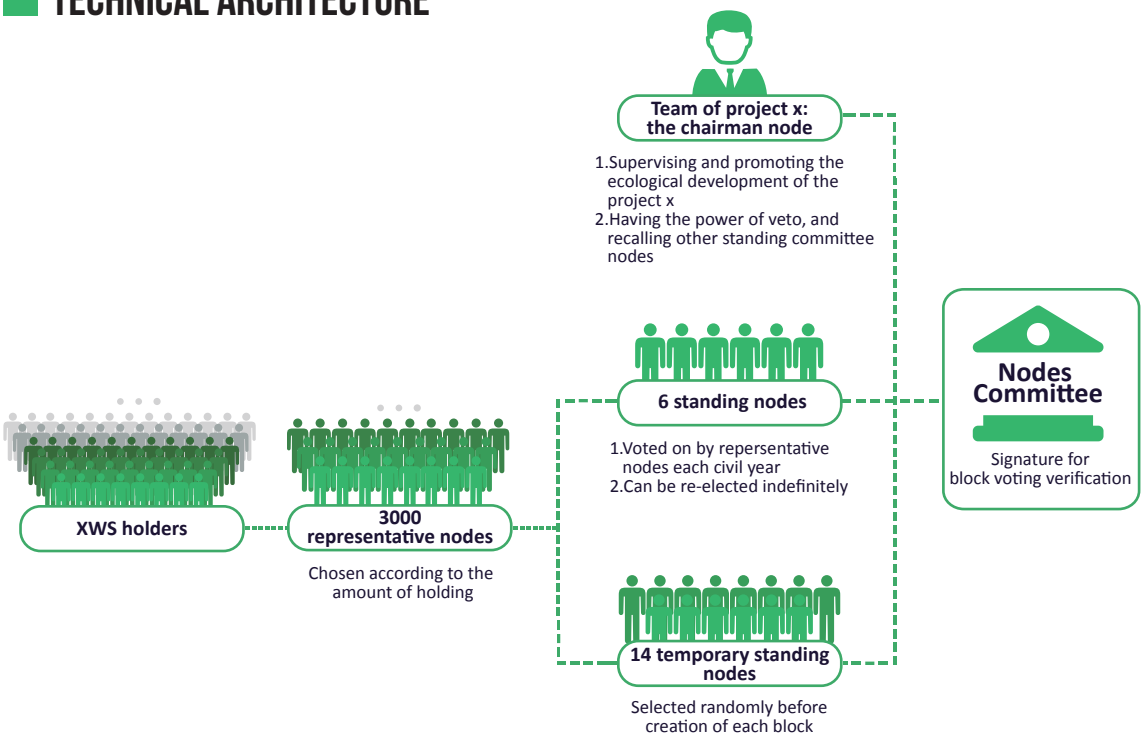
The white X chain consensus algorithm is an improved version of the dpos consensus algorithm, which we call the xpos consensus algorithm. Each account holding XWS is recognized as a basic node, and the top 3000 nodes with the most XWS are automatically selected as the representative nodes. Before each block is created, 14 temporary member nodes will be randomly selected from the 3000 representative nodes; a node representative meeting will be held in each natural year, and 3,000 representative nodes will vote for 6 standing committee members. The project party itself will also serve as a standing committee member to promote and supervise the ecological health development of the project.

The standing committee member nodes will be re-elected for each natural year and can be reappointed consecutively. The standing committee member nodes appointed by the project party serves as the chairman node and has the power of one vote veto and the power to exempt the duties of other standing committee member nodes. The chairman node has no motivation and possibilities for doing evil, because it does not match the intrinsic motivation and position of building a good project ecology.

The 7 standing committee member nodes and 14 temporary committee member nodes form a node committee, and the node committee performs block voting signature verification. When a block is voted by more than 15 node committee members, it will be finalized, which is irreversible. If the temporary member node is malicious, it will be marked as a malicious node. It will lose the account assets and will never be selected as a representative node in the future. If the standing committee member node is malicious, the representative node voters may not vote for it at the next node representative meeting. If the circumstances are serious, the chairman node may exempt it from the standing committee member position.

Unlike the traditional DPOS consensus mechanism, the white X chain divides the entire consensus mechanism into two steps, namely “initiation” and “agreement”. At the beginning of the first step, the system will specify the node signature of the last block that was dug out on the black X chain and initiate a new block. This process can be very fast because the node is most likely to be running and working normally. In the second step, the node committee will act as the verifier and publish its public key. The 21 node committee members will reach a consensus and sign. Then new blocks are generated.

TECHNICAL ARCHITECTURE



The consensus mechanism of the black X chain is the random POW mining mode. In order to conform to the extreme liberal philosophy of the black X chain, the black X chain does not use the traditional SHA256 algorithm for encryption. Instead, it uses the Equihash algorithm to distribute mining, and adjust the number of random nodes involved in mining (these nodes are selected by the algorithm from all miners after the generation of the previous block) automatically according to the calculation difficulty to avoid the occurrence of super miners.

In order to balance efficiency and improve the scalability of the chain, the black X chain designed a cross-chain fragmentation consensus algorithm. The nodes in the block use the computing nodes of the black X chain itself. Even if the number is small, a strong consensus can be achieved. And the node group outside the fragment that is not involved in the actual calculation (that is, the node group composed of the white X chain node and the black X chain node) can also verify the execution process of the calculation by using a simple method. That is to say, it can be verified using mathematical methods without performing the calculation task itself.

The double-stranded chains are interconnected, competing, and interdependent. Due to the participation in the process of initiating and verifying the blocks, the stability of the double-stranded chain system is greatly guaranteed.

3.2 SELECT NODES USING VERIFIABLE RANDOM FUNCTION VRF

TECHNICAL ARCHITECTURE

In the double-stranded chain, the verifiable random function VRF is used to select random nodes for block production. VRF is a consensus framework and a mathematical tool. The ideal consensus algorithm should balance randomness and efficiency. VRF is the best way to solve this contradiction. A perfect VRF has strict randomness, unpredictability, uncontrollability and other security features. It can be non-interactive, which meads low cost and high efficiency.

The essence of the consensus algorithm is how to select one or more nodes to become bookkeepers in a distributed network. Project X's solutions for transaction processing and contract calculation are based on VRF (Verifiable Random Function). VRF is a consensus framework and a mathematical tool.

$$VRF \text{ is a triple:}$$

$$VRF = \{ Generate, Evaluate, Verify \}$$

Here, Generate, Evaluate, and Verify are all polynomial time algorithms. In which,

$$VRF.\ Generate(1^{\gamma}) \rightarrow \{ PK, SK \}$$

VRF. Generate create a pair of PK（public key） and SK (secret key) based on a safety coefficient γ.

VRF.Evaluate generates the corresponding output δ and proof π based on the private key SK and an input x :

$$VRF.\ Evaluate(SK, x) \rightarrow \{\delta(SK, x),\ \pi(SK, x)\}$$

Verifiers can use VRF.Verify to verify the results:VRF. Verify(PK, x, δ, π) → (true|false)

VRF. Generate and VRF. Verify are both probabilistic, and VRF. Evaluate is deterministic.

For any three functions defined on the integer field:

$$a : \mathbb{N} \rightarrow \mathbb{N} \cup \{*\}$$

$$b : \mathbb{N} \rightarrow \mathbb{N}$$

$$s : \mathbb{N} \rightarrow \mathbb{N}$$

And $a(\lambda)$, $b(\lambda)$, $s(\lambda)$ can all be calculated in the polynomial time for λ. We call VRF = {Generate, Evaluate, Verify} is a verifiable pseudo-random function with an input length of $a(\lambda)$, an output length of $b(\lambda)$ and security degree of $s(\lambda)$. The following properties need to be satisfied:

1) (Probability Correctness) The probability for the following two conditions to be correct should not be less than $1\text{-}2^{-\Omega(\lambda)}$:

a) Domain Range Correctness:
For any $x \in \{0,1\}^{a(\lambda)}$, $\delta(SK,x) \in \{0,1\}^{b(\lambda)}$

b) Complete Provability:
For any $x \in \{0,1\}^{a(\lambda)}$, if (δ,π) = VRF. Evaluate(SK,x), then

$$Prob[V(PK,x,\delta,\pi)=true]>1-2^{-\Omega(\lambda)}$$

The left side is the probability of random event V

2) Unique Provability:
For any PK, x, δ_1, δ_2, π_1,π_2, $\delta_1 \neq \delta_2$, then for any i, there exists:

$$Prob[V(PK,x,\delta_i,\pi_i)=true]<2^{-\Omega(\lambda)}$$

3) Residual Pseudorandomness:
For any piar of algorithm $T = (T_C T_d)$, when taking 1^λ as the inital input, and the total number of executions is less than $s(\lambda)$, for $* \neq x$, if:

$$(x,\tilde{\pi}) \leftarrow T_E^{VRF.Evaluate(SK^*)}(1^\lambda, PK)$$

where, PK, SK are generated by VRF. Generate. For a random event X, its probability distribution:

$$\text{Prob}[X:\tilde{\delta}=\delta(SK,x)]=0.5$$
$$\text{Prob}[X:\tilde{\delta}\overset{R}{\leftarrow}(0,1)^{b(\lambda)}]=0.5$$

Then for any guessing algorithm T_d, there exists:

$$\text{Prob}[T_J^{VRF.Evaluate(SK^*)}(1^\lambda, \bar{\delta}, \tilde{\pi}) = X] \leq 0.5 + s(\lambda)^{-1}$$

It can be proved from above that VRF mathematically defines a perfect random number generator, which can be applied to the selection of nodes and the generation of checkpoints in the blockchain system. It is an excellent scheme for randomly selecting accounting miners.

However, in addition to the above three properties of probability correctness, unique provability, and residual pseudorandomness, the random number in the blockchain system should also be unpredictable. Once the book miner is exposed when the bookkeeping has not yet been completed, it is possible to encounter an attack from the perpetrator and cause the book to fail.

Therefore, there is a need for a Verifiable Unpredictable Function (VUF), which is also a triple:

VUF = {Generate, Evaluate, Verify}

The definition of VUF is exactly the same as VRF, and it satisfies the two properties of probability correctness and unique provability in VRF. In addition, it needs to satisfy the unpredictability, that is, for any algorithm T, similar to pseudo-randomness, For $*\neq x$ there must be:

$$\text{Prob}[\ T^{VRF\ .Evaluate(SK^*)}(1^\lambda, PK) = \delta\ (SK, x)] \leq s(\lambda)^{-1}$$

For more information on how to derive VRF for unpredictability, please refer to the paper Verifiable Random Functions published by S. Micali in 1999, which will not be further discussed in this white paper.

3.3 USING ZKSNARK TO ENSURE STRONG ANONYMITY

In order to maintain strong anonymity and protect privacy, the black X chain uses zkSNARK, a simple non-interactive zero-knowledge proof mechanism that treats transactions and contracts (essentially computational tasks) as a logical loop. By encoding the calculations into loop, and generate a proof statement to the verifier, it uses a non-interactive way to verify whether a computing task is actually executed.

IzkSNARK, short for zero-knowledge succint non-interactive arguments of knowledge, refers to a proof structure that proves that someone has certain information. zkSNARK is a zero-knowledge verification technique that is well-suited for blockchains, allowing others to verify the validity of a transaction (or a smart contract function call) without knowing the specific transaction content. With zkSNARK, it not only maintains the consensus between the blockchains and the untrustworthy individuals, but also protects the transaction privacy.

A zero-knowledge proof allows a party (the prover) to prove to the other party (the authenticator) that a statement is true without disclosing any information other than the validity of the statement itself. For example, given a hash of a random number, the prover can convince the authenticator that a number with this hash value does exist, without specifying what the number is.

The succint zero-knowledge proof can be verified in a few milliseconds. Even for statements involving very complex items, the proof length is only a few hundred bytes. In the first generation of zero-knowledge protocol, the prover and the verifier must communicate back and forth, but in a non-interactive structure, the proof contains only a single message sent from the prover to the verifier. Currently, to generate non-interactive, short-lived zero-knowledge proofs that can be published to the blockchain, the only known method is the initial setup phase, which generates a common reference string shared between the validators. We use this public reference string as a public parameter of the system.

If someone has access to the secret randomness used to generate these parameters, they will be able to create false proofs that are valid for the verifier. For Project X, this means that a malicious party can make counterfeit money. To prevent this situation, Project X generates public parameters through a well-designed multi-party communication protocol.

3.3.1 Homomorphism Hiding

Homomorphic hiding is the core technology of zkSNARK in Project X.

If the function $E(x)$ satisfies the following three conditions, we call it the additive homomorphism.

1) For most x, it is usually difficult to solve x for a given $E(x)$.
2) Different inputs will get different outputs - so if $x \neq y$, then $E(x) \neq E(y)$.
3) If someone knows $E(x)$ and $E(y)$, then he can generate x and y in the arithmetic expression. For example, they can use $E(x)$ and $E(y)$ to calculate $E(x+y)$.

Similarly, you can define multiplicative homomorphisms or even full homomorphisms. Note that here the $E(x)$ calculation is done in a finite field, which is hereinafter referred to as Fp. Through homomorphism hiding, a zero-knowledge proof can be achieved to some extent.

A has two secret numbers x and y. It needs to prove to B that the sum of these two numbers is 7. You only need to perform the following three steps:

1) A calculates $E(x)$, $E(y)$ and sends it to B
2) Since the function $E(x)$ satisfies the additive homomorphism, B can calculate $E(x+y)$ by $E(x)$, $E(y)$
3) B independently calculates $E(7)$ and verifies $E(x+y)=E(7)$

3.3.2 Polynomial blind verification

Using the characteristics of additive homomorphism, zero-knowledge proofs can be generalized into polynomials.

Suppose A knows a polynomial P with the highest time d, and B wants to know $E(P(s))$ corresponding to a certain s.

$$P(X)\ a=_0+a_1\cdot X+a_2\cdot X^2+\cdots+a_d\cdot X^d$$

In the ideal verification process, A only knows P but does not know s. B only knows s, but does not know P. This can be achieved by the following means:

1) For each index of s, B calculates $E(1)$, $E(s)$,..., $E(sd)$ and sends it to A.
2) A knows all the coefficients of the polynomial, so he can use the homomorphic property to calculate $P(s)$ and send it back to B.

3.3.3 KCA and complete polynomial blind verification

The polynomial blind verification method mentioned above has a fatal problem, that is, B can't verify that A is actually using the polynomial $P(s)$ to calculate the result. That is to say, it can't be proved that A really knows this polynomial $P(X)$, so the verification above needs to be improved.

Firstly we should define a concept: α pair refers to a pair of values (a, b) that satisfy $b = \alpha * a$. Note that the multiplication here is actually the multiplication on the elliptic curve (ECC). The operation on the elliptic curve conforms to two characteristics. Firstly, when the value of α is large, it is difficult to calculate α through a and b. And secondly, addition and multiplication satisfies the characteristics of the commutative group, which means that the addition and multiplication commutative equations are also true on the elliptic curve.

Using the characteristics of the α pair, we can construct a process called KCA (Knowledge of Coefficient Test and Assumption).

1) B randomly selects an α to generate α pairs (a, b). α saves for itself and send (a, b) to A
2) A selects γ, generates $(a', b') = (\gamma \cdot a, \gamma \cdot b)$, and then returns (a', b') to B. By using the commutative law, it can be proved that (a', b') is also an α pair, $b' = \gamma \cdot b = \gamma\alpha \cdot a = \alpha(\gamma \cdot a) = \alpha \cdot a$’
3) B check (a', b'), confirm that it is α pair, and then assert that A knows γ
   This proof can be generalized to multiple alpha pairs scenarios, which is called d-KCA.
4) B sends a series of α pairs to A
5) A uses $(a’,b’)=(c1 \cdot a1+c2 \cdot a2, c1 \cdot b1+c2 \cdot b2)$, $(a',b')=(c1 \cdot a1+c2 \cdot a2, c1 \cdot b1+ C2 \cdot b2)$ to generate a new α pair
6) B verifies it and asserts that A knows the c array

A complete polynomial blind verification process is as follows

1) Because the multiplication of the elliptic curve conforms to the homomorphic hidden property, A and B can jointly select $x \cdot g$ as E(x)

2) B calculates g, $s \cdot g$,..., $sd \cdot g$ and $\alpha \cdot g$, $\alpha s \cdot g$,...,$\alpha sd \cdot g$ and sends it to A. In fact, the process is the same as the first step of the previous chapter, except that $E(x)$ is substituted into multiplication, increasing the corresponding polynomial result of αs
3) A calculates $a=P(s) \cdot g$, $b=\alpha P(s) \cdot g$ and returns
4) The value of a is the $E(P(s))$ result of the required verification of B, and KCA guarantees that the value of a must be generated by polynomial.

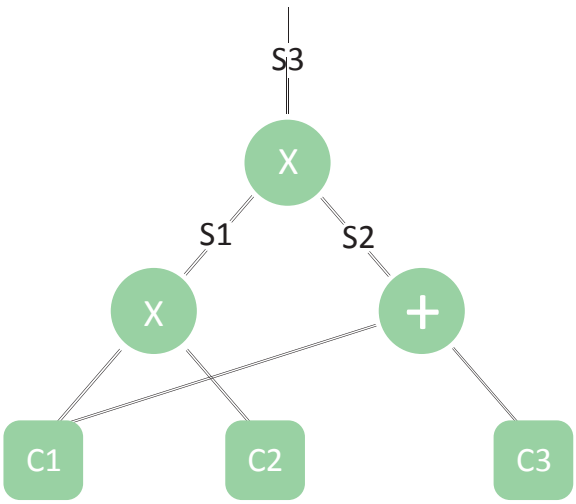
To sum up, we can achieve additive hiding by using additive homomorphism. It allows B to check the value of $x+y$ without knowing x and y. Furthermore, by polynomial blind verification, it is possible to let B check the $P(s)$ for any given s without exposing the polynomial $P(X)$.

The next thing to do is to extend from polynomial to blind verification of arbitrary calculations.

zkSNARK is mainly implemented by the following technologies.

3.3.4 The proof of arbitrary calculation conversion to polynomial

Suppose A needs to prove to B that he knows $c1$, $c2$, $c3$, and that $(c1 \cdot c2) \cdot (c1+c3)=7$. By convention, $c1$, $c2$, $c3$ need to be kept secret to B. The first step we have to do is to "slap the calculation" and use the basic operators to draw the original calculation into such a "calculation gate".



It is also possible to express the formula as $S1=C1*C2;\ S2=C1+C3;\ S3=S1*S2$. By adding intermediate variables, we flatten the complex calculations and use the simplest gate representation. The new gate is equivalent to the original calculation.

In the second step, each gate is represented as an equivalent vector dot product form. This process is called R1CS (Rank-1 Constraint System).

For each gate, we define a set of vectors (a, b, c) such that $s.a * s.b - s.c = 0$, where s represents the vector of all inputs, that is, $[C1, C2, C3, S1, S2, S3]$. In order to allow the addition gate to be expressed in the same way, we add a virtual variable to one, and then the s vector becomes $[one , C1, C2, C3, S1, S2, S3]$.

Corresponding to the first gate, $a=[0,1,0,0,0,0,0];\ b=[0,0,1,0,0,0,0];c=[0,0,0\ ,\ 0,\ 1,\ 0,\ 0]$. Substituting $s, a, b,$ and c into $s.a * s.b - s.c = 0$ yields $C1*C2-S1=0$, that is, the vector expression is completely equivalent to the first gate. Similarly, the second gate $a=[1,0,0,0,0,0,0];\ b=[0,1,0,1,0,0,0];\ c=[0,0\ ,\ 0,0,0,1,0]$ and the third gate $a=[0,0,0,0,1,0,0];\ b=[0,0,0,0,0,1,0\ ];c=[0,0,0,0,0,0,1]$.

Then the vector expression is represented as a polynomial, which converts the verification of the vector into a polynomial verification. This process is called QAP (Quadratic Arithmetic Programs).

The specific method is to select any three different values on the Fp. For example, we select $1, 2, 3$, and find a set of polynomials.

$$a=\left[P_{a1}(x),P_{a2}(x),P_{a3}(x),P_{a4}(x),P_{a5}(x),P_{a6}(x),P_{a7}(x)\right]$$
$$b=\left[P_{b1}(x),P_{b2}(x),P_{b3}(x),P_{b4}(x),P_{b5}(x),P_{b6}(x),P_{b7}(x)\right]$$
$$c=\left[P_{c1}(x),P_{c2}(x),P_{c3}(x),P_{c4}(x),P_{c5}(x),P_{c6}(x),P_{c7}(x)\right]$$

so that when x takes the value $1, 2, 3$ respectively, the a, b, c arrays take value corresponding to the vectors of the above three gates.

The problem translates into retrospecting a polynomial definition by a known solution, which can be done using Lagrangian interpolation. In this process, Lagrangian interpolation is needed for each value of the vector. For complex problems, this vector will be very large, and the calculation process will be very complicated. Here, the Fast Fourier Transform can be used for optimization.

Here, the original three vector groups are represented as an array $a(x)$, $b(x)$, $c(x)$ represented by x. Take the polynomial $P(x)=s.a(x) * s.b(x) - s.c(x)$. According to the original definition, when x is 1, 2 or 3, $P(x)=0$. According to the polynomial property, $P(a)=0$ is equivalent to that P can be divisible by $(x-a)$, and $P(x)$ must be divisible by $(x-1)(x-2)(x-3)$. That is, there exists $H(X)$, such that $P(x)=T(x)*H(x)$, where $T(x-)=(x-1)(x-2)(x-3)$.

Note that the QAP process converts the values of the original three points into a polynomial, which is equivalent to inserting a lot of meaningless values in the middle. The values of these values are independent of the original formula. That is to say, the verification of the polynomial is not equivalent to the verification of the original calculation, but the verification of the polynomial also verifies the meta-calculation.

The proof of the final original expression is transformed into a proof of polynomial. As long as $P(x)=T(x)*H(x)$ is proved, the original formula can be verified.

3.3.4 Pinocchio Agreement

Through QAP, the proof of the formula has been converted into a proof of polynomial. The following is a complete verification process.

To simplify the description below, we define s . $a(x)$ as $L(x)$, s . $b(x)$ as $R(x)$, s . $c(x)$ as $O(x)$, then the equation to be proved can be rewritten as $L(x)*R(x)-O(x)=T(x-)*H(x)$. The highest order of L, R and O is d, so the highest order of this equation is $2d$, and the number of two inequality polynomial intersections is only $2d$ at most. When $2d$ is small as compared with the number of elements of finite field p, we can use the sampling method to verify that the equivalence of the polynomials. The probability that the polynomial $P(x)$ randomly selected by A is verified is only $2d/p$. The process of random sampling and verification is as follows:

1) A Select the polynomial L, R, O, H according to the previous chapter.
2) B select random point s and calculate $E(T(s))$
3) A calculates $E(L(s))$, $E(R(s))$, $E(O(s))$, $E(H(s))$ $(E(s), E(s2)$ according to B ,...)
4) B test $E(L(s)*R(s)-O(s))=E(H(s)*T(s))$

There are four more issues to be solved in this proof process:

3.3.4.1 Ensure that L, R, O are generated from the same set of parameters s

There is a flaw in this proof process, as we define $L(x)=s\,.\,a(x)$, $R(x)=s\,.\,b(x)$, $O(x)=s\,.\,c(x)$, here hides a limitation that L, R and O must be generated by the same vector s, which is ignored in the proof. That is to say, A can cheat by selecting a polynomial that does not meet this qualification. The solution is still KCA, but this time the KCA is more complicated.

Firstly we define two formulas:

$$F=L+X^{d+1}\cdot R+X^{2(d+2)}\cdot O$$

$$F_i=L_i+X^{d+1}\cdot R_i+X^{2(d+2)}\cdot O_i$$

The meaning of this formula is to stagger the exponents of L, R, and O. If L, R, and O are actually generated from the same group of $s=[s1,....sm]$, there must be

$$F=\sum_{i=1}^{m} c_i\cdot F_i$$

In other words, as long as A can give a linear combination of F and Fi, it can be proved that L, R, O meet the qualification conditions. This qualifying problem translates into a d-KCA problem.

1) B selects the hidden α, calculates $E(\alpha*Fi)$ and sends it to A.
2) A calculates $E(\alpha F)$ and sends back to B
3) B calculates $E(F)$ and verifies α pair according to the formula of this paper.

3.3.4.2 Prevent brute force cracking

In the current process, A needs to put $E(L(s))$, $E(R(s))$, $E(O(s))$, according to the characteristics of the homomorphic hidden, these values can not retrodict the original polynomial. However, if there are not many solutions to the needed verification, B can still violently crack the original problem by exhaustive means and get the original data of A. For example, we know that A has two positive integers, which requires blind verification that the product of these two positive integers is 12, then B can completely exhaust the product of all positive integer combinations of 12, and perform the verification process in the forward direction, and compare with $E(L(s))$, $E(R(s))$ and $E(O(s))$ to know what the correct answer is.

For brute force cracking, the solution of Project X is to introduce random offset when generating L, R, O.

$$L_z:=L+\ \delta_1\cdot T, R_z:=R+\delta_2\cdot T, O_z:=O+\delta_3\cdot T$$

because

$$\begin{aligned}&L_z\cdot R_z-O_z=(L+\delta_1\cdot T)\cdot(R+\delta_2\cdot T)-(O+\delta_2\cdot T)\\&=(L\cdot R-O)+L\cdot\delta_2\cdot T+\delta_1\cdot T\cdot R+\delta_1\delta_2\cdot T^2-\delta_3\cdot T\\&=T\cdot(H+L\cdot\delta_2+\delta_1\cdot R+\delta_1\delta_2\cdot T-\delta_3)\end{aligned}$$

define

$$H_z:=H+L\cdot\delta_2+\delta_1\cdot R+\delta_1\delta_2\cdot T-\delta_3$$

The new combination L_z, R_z, O_z, H_z can still pass the polynomial test, and because B does not know the random number, it can't know the original parameters by brute force cracking.

3.3.4.3 Multiplication homomorphism

In the final step of the Pinocchio agreement, B needs to verify $E(L(s)*R(s)-O(s))=E(H(s)*T(s))$, and in fact, the above only mentions that $E(x)$ satisfies the addition homomorphism, but B cannot calculate $E(H(s)*T(s)$ by $E(H(s))$.

The elliptic curve pairing feature is needed to solve this problem. Through elliptic curve pairing, we can get a weakened version of the multiplicative homomorphism.

We define $E1(x):=x\cdot g$, $E2(x):=x\cdot h$, $E(x):=x\cdot g$. Because all three functions are elliptic curves, they naturally conform to the additive homomorphism. The curve matching feature of the ellipse ensures that we can calculate $E(xy)$ from $E1(x)$, $E2(y)$.

3.3.4.4 Reduce interaction

The last and most critical issue is that the Pinocchio protocol requires a lot of message interaction between A and B, and in the blockchain, what we want to do is "public certification." The ideal situation is that as long as A puts the evidence as a string on the chain, anyone can verify the conclusion.

However, the fact is that this zero-interaction proof in the strict sense has proved to be incapable of satisfying all proof scenarios. We have to take the second best and use a method called CRS (Common Reference String). The principle is very simple, that is , to build the random numbers α and s into the “system".

So the final zkSNARK process is:

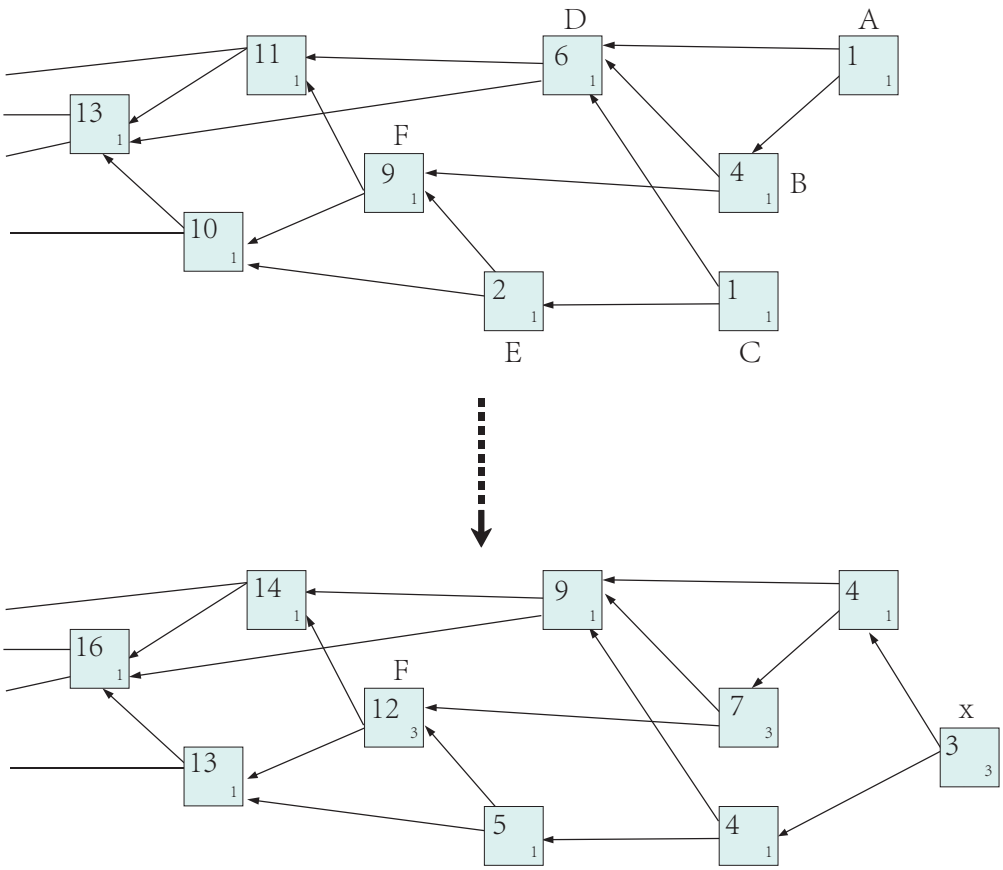
1) Configure α and s to calculate $(E1(1), E1(s),..., E1(sd), E2(\alpha), E2(\alpha s),...,E2(\alpha sd))E2(\alpha)$, and then publicize them
2) A uses the public parameter to calculate the verification polynomial
3) B checks the polynomial, the multiplicative homomorphic part is completed by the characteristic of elliptic curve pairing, such as $E(\alpha x)=Tate(E1(x), E2(\alpha))$
4) Organize blocks using directed acyclic graphs to avoid bifurcation

3.4 ORGANIZE BLOCKS WITH DIRECTED ACYCLIC GRAPHS TO AVOID BIFURCATION

In order to improve the safety of the X double-stranded chain and solve the bifurcation problem of the longest chain, the X double-stranded chain uses the directed acyclic graph (DAG) organization block. Firstly it determines a pivot chain and then sorts all the blocks; all blocks on the DAG are added to the transaction history to contribute to throughput.

WEIGHTS AND RELATED CONCEPTS

Here, we define the weight of a transaction and its related concepts. The weight of the transaction is proportional to the amount of work invested by the node that sent the transaction; in practice, the weight can be assumed to be some value of $3n$, where n is an acceptable positive integer with a non-empty interval.

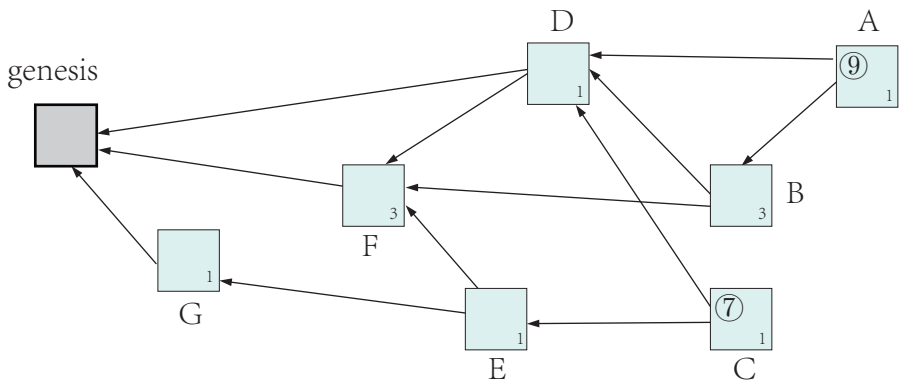


An important symbol we need is the cumulative weight of a transaction: it is defined as the sum of the weight of the transaction itself and the weight of all other transactions that directly and indirectly verify the transaction. The calculation method of cumulative weight is shown in the figure above. The box represents the transaction, the smaller number in the lower right corner of the box indicates the weight of the transaction, and the larger and bolder number is the cumulative weight of the transaction. For example, transaction F is verified directly or indirectly via transactions A, B, C, E. The cumulative weight of transaction F is the sum of the respective weights of transactions A, B, C and E, $i.e. 9 = 3+1+3+1+1$.

The transactions that are not verified *(i.e. "tips")* are only transaction A and transaction C. If a new transaction X enters the system and validates transactions A and C, then transaction X is the only tip in the system, and the weight of all other transactions in the system is increased by 3 ($i.e.$ the weight of transaction X itself).

To discuss the verification algorithm, we need to introduce some other variables. First, for a vertex in a tangling (for example, a transaction), we introduce:

- Height, defined as the longest length of all paths from the first transaction to the current transaction.
- Depth, defined as the longest path from this transaction to the top of a tip.



For example, in the figure above, the transaction G has a height of 1 and a depth of 3 (because of the reverse path F, B, A); while the transaction D has a height of 2 and a depth of 2 (Translator's Note: According to this version's definition of height and depth in the paper, the translator considers the height to be 3 and the depth to be 2; for height and depth, please refer to the author's latest definition of the paper submitted to Ledger magazine). Next, we introduce the sign of the integral. The integral of a transaction is defined as the sum of its own weight and the weight of all the transactions it verifies. Similarly, the only tips are transactions A and C. Transaction A directly or indirectly verifies the trades B, D, F, G, so the trade A's score is $1+3+1+3+1=9$. Similarly, the score for transaction C is $1+1+1+3+1=7$.

WEIGHTS AND RELATED CONCEPTS

Let $L(t)$ be the total number of tips in the system at time t. Of course, everyone expects the random variable $L(t)$ to remain stable (more precisely, recursively). Intuitively, $L(t)$ should fluctuate around a constant rather than tend to infinity (so there will be a large number of unverified transactions in the system).

In order to analyze the stability of $L(t)$, we need some assumptions. Let λ be the rate of the transaction input stream (Poisson distribution); for simplicity, we assume that the rate of the transaction input stream remains constant. Assume that all devices have roughly the same computing power; and assume that the total number of transactions in the system is N, and in the case of L unverified cases, the average time required for a device to send a transaction is $h(L, N)$. First, we consider a strategy in which the node randomly selects two of the L tips and verifies them when a transaction is to be sent. Under this strategy, it can be assumed that the verification of different tips is independent of each other, then there is a rate λ / L (refer to the theorem *5.2 in [5]*). Therefore,

$$P[\text{no transaction for a given tip in } h(L,N) \text{ time}] = exp(-\frac{\lambda h(L, N)}{L}) \quad (1)$$

This means that when our device initiates a transaction, the expected increase in the total number of tips is equal to

$$1 - 2exp(-\frac{\lambda h(L, N)}{L}) \quad (2)$$

In the above formula, *"1"* corresponds to the new tip created by this transaction, and the second item is the expected value of the "erased" tips. It can now be seen that $L(t)$ is actually a continuous random walk that converts between neighbors in space $N=\{1, 2, 3,...\}$. If the two selected transactions have been verified by other transactions, then the process will go one step to the left; if the two selected transactions are not verified, then the next step is to the right; The last possibility outside is to stay in place.

Next, to understand the general behavior of this process, we notice that the drift term in equation *(2)* is positive for L when it is small, and negative for L when it is large (at least for $L \to$, $h(L, N) = o(L)$; or just assume that the main contribution to the calculation and transaction diffusion is not from the processing of the tips). When the formula *(2)* approaches zero, L obtains a typical value, that is, L_0.

$$L_0 \approx (-\frac{\lambda h(L_0,N)}{ln2}) \approx 1.44\lambda h(L_0,N) \quad (3)$$

Obviously, the L_0 defined above is also the typical number of tips. At the same time, the time required for a transaction to be verified for the first time is estimated to be

$$L_0 / \lambda$$

At the same time, note that (at least in the case of trading nodes trying to verify the tips) for any fixed t time, those tips constitute a truncated set in a certain phase

$$s \in [t, t + h(L_0, N)]$$

meaning that any transaction initiated at time $t' > t$ that goes to the founding transaction must pass this collection. At least in some accidental cases, the size of this truncated set becomes very small, which is extremely important. We may be able to use this smaller truncation set as a checkpoint, as a possible pruning of the DAG or for other purposes.

The above "pure random" strategy is not very good in practice because it does not encourage nodes to verify transactions: for example, "lazy" users may always verify several earlier fixed transactions (and therefore does not contribute to the verification of latest deals), and this behavior will not be punished. To eliminate this type of behavior, we need to adopt a strategy to bias new transactions toward verifying those with higher scores.

The following is an example of the above strategy. Pick a fixed parameter $\alpha \in (0,1)$ and then arbitrarily select two transactions based on the integral of the tips in the middle of the first αL tips. Perform the same analysis as the case in the previous strategy, you can get the typical size of this tips collection as

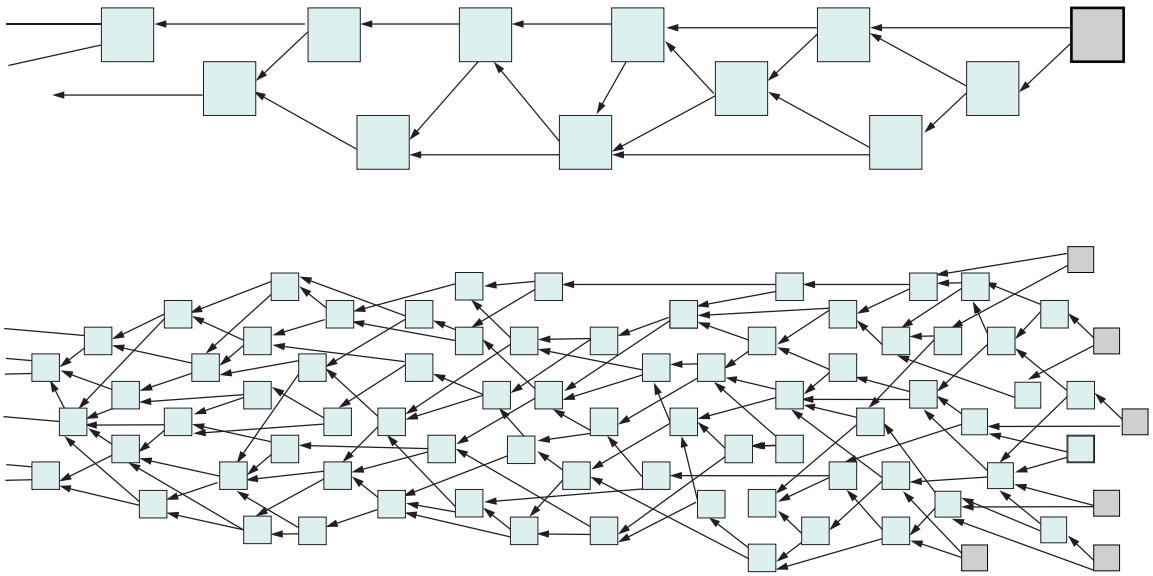
$$L_0^{\alpha} \approx \frac{\lambda \mathrm{h}(L_0, N)}{\alpha \ln 2} \approx 1.44\alpha^{-1}\lambda h(L_0, N) \quad (4)$$

Therefore, in this case, it is a bit more complicated to solve the expected value of the time required for a transaction to be verified for the first time. We analyze in two intervals, as shown in the figure below.

• Low load area: The transaction flow is slow enough, so even if the number of tips is quite small, it is unlikely that different transactions will verify the same tip.

• High load area: The transaction flow is large enough, so the tips remain large.

In the low-load area, this situation is relatively simple: the first verification occurs on the time scale, because the first (or one of the first) incoming transactions will validate our transactions.



The figure above Tangles and their typical tip set (boxes with shadows) under low load and high load conditions. It should be noted that under high load conditions, some transactions may need to wait a long time to get the first verification.

Now let's consider the situation in the high load area. First, for those transactions that do not enter the top αL tip, their wait time will be very long, and probably takes the time scale of $\exp(cL_0^{(\alpha)})$ (because for smaller L values, there is a tendency to offset to $cL_0^{(\alpha)}$, while the size of the tip is set to be smaller than $cL_0^{(\alpha)}$ so that there is a chance to be verified). Therefore, in this case, a better strategy is that the sender of the transaction resends a blank transaction that points to the previous transaction and verifies it, and hopes that the new transaction will enter the top αL tip. Similarly, another easier strategy is to choose, for instance 5 random tips (select among all the tips), and then verify the first 2 tips of the 5 tips. Similarly, if your transaction is not verified within the time scale of $\Theta(L_0 / \lambda) = \Theta(\mathrm{h}(L_0, N))$, a good idea is to initiate a new blank transaction to verify and promote the transaction.

We also noticed that the above verification strategy can be further improved to prevent spam attacks. For example, a node may prefer to verify those tips that have a greater weight on their own, making it less likely for an attacker's spam transaction to be verified.

In the low-load area, after the transaction is verified several times, its cumulative weight will increase at a rate of λw , where w is the average weight of a normal transaction, because essentially all new transactions will indirectly point to our transaction.

In the high load area, as observed above, if the transaction is old enough and has a large cumulative weight, then the cumulative weight will increase at the same rate of λw . Of course, we can see that the transaction needs to wait a certain amount of time to be verified at the beginning, and it is clear that its cumulative weight will initially grow in a more random form.

In order to understand the behavior of a cumulative weight change after a transaction being verified, we define $H(t)$ (for simplicity, we start timing from the creation of the transaction) as the cumulative weight expectation of the transaction at time t, and uses $K(t)$ to indicate the expected value of the number of tips for verifying the trade at time t. Here in brief, we note $h := h(L0,N)$. Meanwhile, we make a simplifying assumption that the total number of tips is generally constant (equal to $L0$). Here we use the strategy of “randomly verifying two tips”; the results are expected to be roughly the same as those obtained by “randomly verifying the two tips in the top αL tips” strategy.

A transaction entering the system at time t is usually the state of the system at time t-h to select two transactions for verification. It is not difficult to obtain the conclusion that the probability to verify at least one tip is $\frac{K(t-h)}{L_0}\left(2-\frac{K(t-h)}{L_0}\right)$. Consequently, we can write the following differential equation (similar to example 6.4 in *[5]*):

$$\frac{dH(t)}{dt}=w\lambda\frac{K(t-h)}{L_0}\left(2-\frac{K(t-h)}{L_0}\right) \qquad (5)$$

In order to be able to use equation *(5)*, we first need to calculate $K(t)$. It is difficult to calculate $K(t)$ immediately because a tip at time t-h may not be the tip at time t, and if the newly entered transaction verifies such a tip, then total number of tips verifying the original transaction will increase by one. Now according to *(1)* and *(3)*, it is observed that the probability that a tip at t-h remains a tip at time t is *1/2*. Therefore, at time t, half *(i.e., K(t-h))* of the "previous" tips remain as tips while the other half have been verified by at least one transaction. Let us use A to indicate (probably) that $K(t\text{-}h)/2$ tips at t-h is still a collection of these transactions for tips at t, and B indicates the other half of the tips that have already been verified. Assume that the probability of the newly entered transaction verifies at least one transaction in set B without verifying any transaction in set A is $p1$; it is also assumed that the probability of simultaneous transactions verification in set A and set B is $p2$. Obviously, $p1$ and $p2$ correspond to the probability that the current "our" tips increase or decrease by one when new transactions arrive. So we get some basic relationships:

$$p_1=\frac{K(t-h)}{L_0}\left(1-\frac{K(t-h)}{L_0}\right)-\left(\frac{K(t-h)}{L_0}\right)^2 \qquad p_2=\left(\frac{K(t-h)}{2L_0}\right)^2$$

Similar to equation *(5)*, there is a differential equation for $K(t)$:

$$\frac{dK(t)}{dt}=(p_1-p_2)\lambda=\lambda\frac{K(t-h)}{L_0}\left(1-\frac{K(t-h)}{L_0}\right) \qquad (6)$$

It is still difficult to solve equation *(6)* accurately, so we further simplify the hypothesis. First of all, we can see that for any fixed $\varepsilon>0$, when $K(t)$ reaches the level of εL_0, $K(t)$ will grow rapidly to L_0. Now, when $K(t)$ is relatively small compared to L_0, we can discard the last item on the right side of equation *(6)*. At the same time, we use $K(t)-h\frac{dK(t)}{dt}$ to substitute $K(t-h)$, and we can get the simplified version of equation *(6)* (note that $\frac{\lambda h}{L_0}=\ln 2$)

$$\frac{dK(t)}{dt}=\frac{\lambda}{1+\ln 2}\approx 0.59\frac{\lambda K(t)}{L_0} \qquad (7)$$

The boundary condition is $K(0)=1$. Solving the above differential equation we can obtain

$$K(t) \approx \exp\left(\frac{t \ln 2}{(1+\ln 2)h}\right) \approx \exp\left(0.41\frac{t}{h}\right) \quad (8)$$

Therefore, for the logarithm of *(8)*, the time for $K(t)$ to reach εL_0 is approximately:

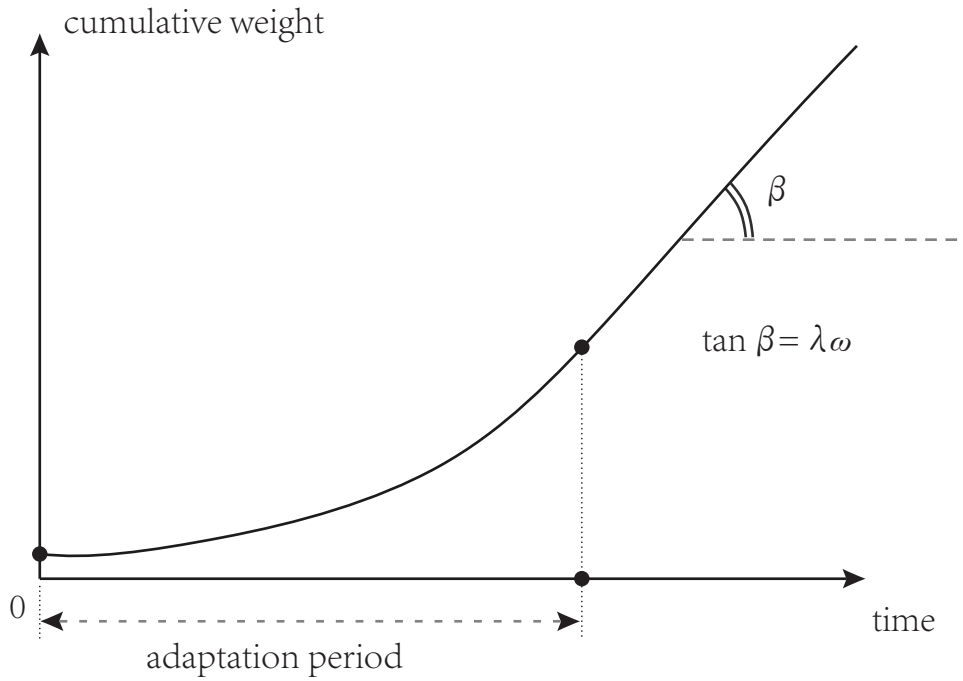
$$t_0 \approx \left(1+(\ln 2)^{-1}\right)h \times (\ln L_0 - \ln \varepsilon^{-1}) \leq 2.44h \ln L_0 \quad (9)$$

Going back to equation *(5)* (discard the last item on the right as previous), we can get the following equation in the "adjustment phase" (for example, for $t \leq t_0$ the result of *(9)*):

$$\frac{dH(t)}{dt} \approx \frac{2w\lambda}{L_0 \exp\left(\frac{\ln 2}{1+\ln 2}\right)} K(t) \approx \frac{2w\lambda}{L_0 \exp\left(\frac{\ln 2}{1+\ln 2}\right)} \exp\left(\frac{t \ln 2}{(1+\ln 2)h}\right)$$

thus,

$$H(t) \approx \frac{2(1+\ln 2)w}{\exp\left(\frac{\ln 2}{1+\ln 2}\right)} \exp\left(\frac{t \ln 2}{(1+\ln 2)h}\right) \approx 2.25w \exp\left(0.41\frac{t}{h}\right) \quad (10)$$



As discussed above, after the adjustment phase, the cumulative weight $H(t)$ will increase linearly with speed λ_W. What we need to emphasize is that the exponential growth in *(10)* does not mean that the cumulative weight will grow rapidly during the adjustment phase. The image is given in the figure above.

At the same time, we believe that the calculations in this section can be easily adjusted if the nodes point to the $s>1$ transactions. In that case, we only have to replace 2 with s in *(2)* (but not in *(5)*), and replace ln 2 with ln s in *(3)*-*(4)* and *(7)*-*(10)*.

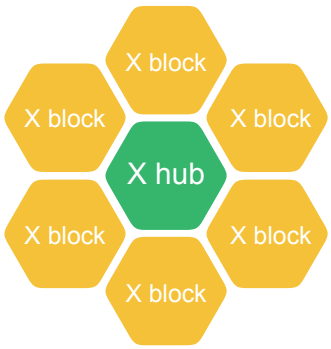
3.5 CROSS-CHAIN TECHNOLOGY

XDC (X-Dimension Communication), i. e. X-dimensional communication technology, can break through the barriers of public-chain communication and realize communication between different public chains. It is a major breakthrough for the Project X team at the cross-chain level, and it also serve as a propellant for double-stranded chain ecology. Nowadays, the existing interconnected blockchain communication (IBC) technology needs to be improved in the process of communication between the twin chain system and the external chain. Based on the fact, the Project X team creatively proposed the concept of the robust balance control of the double-stranded chain, which can greatly improve the stability of the system.

3.5.1 *Interconnected blockchain communication (IBC) technology*

The blockchain on Project X is called the "X zone". Some of these zones are also known as "X Hubs", and different zones can communicate and interoperate with each other through shared hubs. The first zone on the Project X network is the X Hub.

Because all cross-zone token transfers need to be done through the X hub, tokens can be transferred between zones safely and quickly. There is no need for direct exchange liquidity between zones, We only have to track the total amount of tokens held in each zone through the X hub, and to ensure that the total amount of tokens in all zones remains the same. Here, the X hub plays a role similar to the central bank settlement function.



Interconnected Blockchain Communication (IBC) Technology

All cross-block token transfers need to be made through the X hub, and tokens can be transferred between blocks safely and quickly. There is no need for direct exchange liquidity between blocks. We only have to track the total amount of tokens held in each block through the X hub , and to ensure that the total amount of tokens in all blocks remains the same. Here, the X hub plays a role similar to the central bank settlement function.

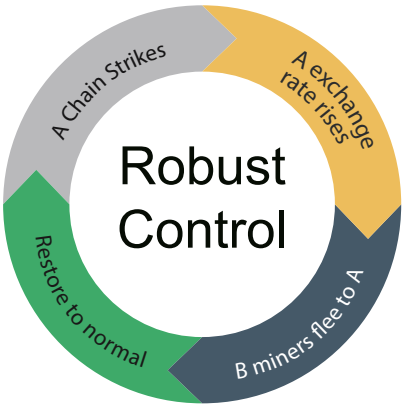
3.5.2 Robust balance control

Project X pioneered the concept of robust balancing between twin chains. Robustness is an important concept in modern control theory, which refers to the ability of the system to maintain stability under various random disturbances. For the blockchain ecology, robustness is crucial. If it is serious, it will directly lead to the bifurcation and formula rupture. For example, the mining difficulty adjustment mechanism in Bitcoin can better ensure the stability of the block-out rate. Bitcoin cash improved the mechanism, and its difficulty adjustment algorithm (DAA) has ensured the stable block-out ability under the small calculation power at the beginning of the bifurcation.

The double-stranded chain system needs to ensure the simultaneous development and mutual benefit. If one of the chains is subjected to malicious attacks, the negative miner block out, or the secondary marketers and speculations, etc., it will inevitably have a major impact on the other chain. Therefore, the twin chain ecosystem requires more robustness and balance, and requires a faster, more stable, and smarter self-adjusting algorithm to maintain the balance of the double-stranded chain ecosystem.

To this end, we draw on the robust control theory and establish the economic and ecological model of the double-stranded chain system. In addition to adjusting the mining difficulty and the block-out rate, it also introduces a dynamic adjustment mechanism of the exchange rate, which allows the tokens to exchange within the chain. Taking the strike of the A chain miner as an example. The double chain loses balance, and at this time, the rapid adjustment between the chains makes the exchange rate of the A chain token gradually increase, so that the mining income of the A chain is higher. The B chain miner will quickly transfer into the A

chain mining, and the A chain can reach a balanced stage in a short period of time, so that the exchange rate is finally adjusted to a normal state and the double-stranded chain ecology is once again balanced. The dynamic exchange rate is calculated according to the optimal control algorithm such as variational method and genetic algorithm to ensure the robustness of the double-stranded chain ecology and form a stable and reliable trading closed-loop ecosystem.



Robust Balance Control

Project X pioneered the concept of robust balancing between twin chains. We draw on the robust control theory and establish the economic and ecological model of the double-stranded chain system. In addition to adjusting the difficulty of mining and the block out rate, we also introduce a dynamic adjustment mechanism of the exchange rate, which allows for the exchange of tokens cross chains. The dynamic exchange rate is calculated according to the optimal control algorithm such as variational method and genetic algorithm to ensure the robustness of the double-stranded chain ecology, and form a stable and reliable trading closed-loop ecosystem.

04
PROJECT ECOLOGY

4.1 XAPP ECOLOGY

Project X's double-stranded chain ecosystem abandons the traditional DApp ecosystem as an application layer, and adopts a new underlying twin chain, that is, XApp's business model architecture. By opening the API of the project integration module to developers and project parties instead of the traditional smart contract module, the XApp module greatly reduces the development difficulty of the project side and the developer, and helps the traditional Internet developers who have ideas but not strong enough to eliminate the high learning costs of smart contracts. It directly introduced projects with high quality values that have not been fully demonstrated to our Project X double-stranded chain ecosystem to create value and change the future of the blockchain ecosystem.

For eligible quality projects, the Foundation will give initial funding and free technical guidance based on the project's prospects, and successful projects will also receive token rewards as incentives. A proportion of the continuous profit generated by the participating project parties will be turned over to the White X Chain Foundation in the form of tax. The Foundation will distribute all taxes to all XWS positions as a dividend in each financial cycle. All the previous public chains have a problem: there is only one-way interaction between the public chain and the application layer, that is, the public chain provides powerful underlying technical support to the application layer, but it cannot obtain effective feedback. In the long term, the bottom layer loses the energy and power of maintenance, which is a very unhealthy mode. Therefore, in the X double-stranded chain ecology, we introduce the concept of taxation, so that the underlying public chain and the application layer are no longer one-way output, but reach mutual benefit and win-win situation to form a benign ecological cycle.

4.2 IXO PLAN

To facilitate the continued development and advancement of blockchain technology, Project X will implement the IXO program at a suitable time to help and support high-quality projects with potential. IXO plans to rely on Project X's white X chain eco-credit endorsement, using the project X team's professional experience and rich resources, aiming at selecting high-quality projects for users, to raise development funds for the project. Users can use XWS to participate in the plan. The IXO program combines the two technical features of the Project X project: X ID and X-dimensional technology.

X ID technology is a new generation of user identity authentication technology developed by Project X team based on multi-source authentication technology. It aims to improve user identification accuracy and ensure the security of users participated in X plan. X ID technology refers to the multi-source authentication of multiple different certifiers from different perspectives and different aspects to a more comprehensive and more diverse identity authentication. The certification done by any authenticator in the X ID technology system is signed by the authenticator and has characteristics such as unforgeable and non-repudiation. At the same time, the authenticator itself can also pass the authentication trust. If there exists any doubt about the authority or trustworthiness of the authenticator, the certification party's qualification or reputation can also be authenticated. This will form a chain of certification and finally form a certification network.

X-dimensional technology refers to the cross-chain technology that allows Project X to break through the constraints of the public chain. Nowadays, the public chain technology is developing rapidly, and there are many excellent public chains. There are also many diverse projects based on these public. However, the incompatibility caused by the different types of public chains has always been an insurmountable scorpion in public chain development. The Project X team will work hard to overcome this problem to achieve interoperability between the public chains. On this basis, the IXO program can ignore the constraints and carefully select all kinds of high-quality projects on the public chain to help users realize value investment and asset appreciation.

4.3 THE GHOST WALLET

The Ghost Wallet is an anonymous wallet Dapp deployed by the Project X team at the black X chain. Ghost is the man of the underworld. The user takes the ship of the soul ferry (X-encrypted anonymous technology), and leads to the ghost country, the underworld, via the Styx. No matter what identity in the world, after entering the underworld (wallet) everyone is a ghost, and their identity cannot be verified or traced. In the wallet, there is a ghost bazaar that follows the absolute anonymity and freedom of the underworld to protect the privacy of users. The products in the market will not be interrogated and intervened.

The anonymous encryption of the ghost wallet is based on zkSNARK technology. zkSNARK is a zero-knowledge verification technique that is well-suited for blockchains, allowing others to verify the validity of a transaction (or a smart contract function call) without knowing the specific transaction content. With the help of zkSNARK, it not only maintains the consensus between the blockchains and the untrustworthy individuals， but also protects the transaction privacy. For details of the zkSNARK technology, please refer to section 3.3 of the white paper.

4.4 SOCIAL RESPONSIBILITY AND PUBLIC BENEFIT

The goal of Project X is to build a blockchain platform that connects the whole world. At the same time, we also have to bear the corresponding social responsibilities. We will use part of the profit for the public welfare undertakings related to the blockchain, especially on the popularization and education of blockchain related knowledge.

The pace of new technology development in today's society is getting faster and faster, and we can clearly feel the promotion of technological progress to the whole society. Computers and the Internet have brought us an information age that has completely changed the way people live. However, we must also note that many people in today's world cannot enjoy the convenience brought by these new technologies because of various objective factors. From this perspective, technological progress is being segregated by different people. As time goes by, people will have a hard time understanding each other, resulting in barriers. This barrier exists in the crowded with different ages, regions, and income levels.

PROJECT ECOLOGY

In the future, social blockchain technology will become an underlying system, and blockchain-related applications will be as popular as computers and the Internet. One of the characteristics of the blockchain is that the cost of information tampering is extremely high. Based on this feature, mutual trust and consensus will be smoother. In the end, it will change the way people think and act, thus promoting the efficiency of the human social collaboration as a whole. However, we believe that the change of the way of thinking and doing things must be based on cognition. Those who do not understand the basic principles of blockchain cannot generate sufficient trust in blockchain technology, and the role of blockchain technology cannot be reflected. In addition, because the traditional media does not have a deep understanding of the blockchain technology, there are certain deviations in the propaganda, which also affects the public's cognitive level of the blockchain. Therefore, Project X is not only about the blockchain technology innovation. We also attach importance to the popularization and education of blockchain related knowledge.

Part of the profit generated by Project X project will be used to establish the Project X Public Welfare Foundation. The main work of the Foundation is as follows:

1) Establish blockchain media and popularize the basic knowledge of blockchain and related application information.

2) Reach in-depth cooperation with traditional educational institutions, promote blockchain courses into colleges and universities, and set up blockchain-related majors to reserve talents for the blockchain industry.

3) Establish a blockchain project incubation fund to provide sufficient resources for blockchain entrepreneurs.

4) Organize blockchain technology competitions or blockchain application exhibitions and other related activities to expand the influence of blockchain technology.

5) Establish blockchain industry associations, formulate blockchain technical standards, establish and improve blockchain industry qualification certification system, and promote standardization and regularization of blockchain industry.

6) Other related matters that are conducive to the development of the blockchain industry.

PROJECT ECOLOGY

From emergence to widespread application, most new technologies in human history requires a long process. Consequently, we can't just focus on the advancement of technology. We must accelerate the application of technology in many ways. We hope that Project X Public Welfare Foundation can raise the public's awareness of blockchain technology, improve the blockchain education system and related standards, and promote the healthy development of the blockchain industry.

05
TOKEN ECONOMY

5.1 DOUBLE TOKEN MECHANISM

5.2 XWS RELEASE PLAN

5.3 THE BUDGET OF RAISING FUNDS

5.4 XWS APPLICATION SCENARIOS AND VALUES

5.1 DOUBLE TOKEN MECHANISM

EOS's practice of infinitely issuing tokens to meet the block reward needs will lead to inflation of the tokens. The double-stranded chains insist that the tokens will never be issued additionally to ensure that the value of the tokens will not be diluted. The block awarded by the white X chain block producer is the black X chain token XBC, and the number of XBC tokens obtained per block is calculated by the double-stranded chain exchange rate protocol developed by the project party. The black X chain uses a similar mining incentive mechanism as Bitcoin, so there is no worry about inflation. Also it helps the white X chain initiation block to receive XWS rewards, and the number is also calculated by the double-stranded chain exchange rate agreement. The interaction between the two chains is controlled by the double-stranded chain cross-chain protocol developed by the project side. Since the white X chain block reward is not a token of its own chain, the token does not have to be additionally issued to cause inflation; while the black X chain block reward also has some tokens that are not on its own chain, the token dug rate is delayed to make mining more sustainable.

In addition, since the block reward of the white X chain is the token XBC of the black X chain, the node that does not have the position of the position will not be strong because it continues to act as the verification node, so that more nodes can be given to the subsequent nodes. The opportunity to be elected as a node is also a big advantage of the interaction between the two chains.

5.2 XWS RELEASE PLAN

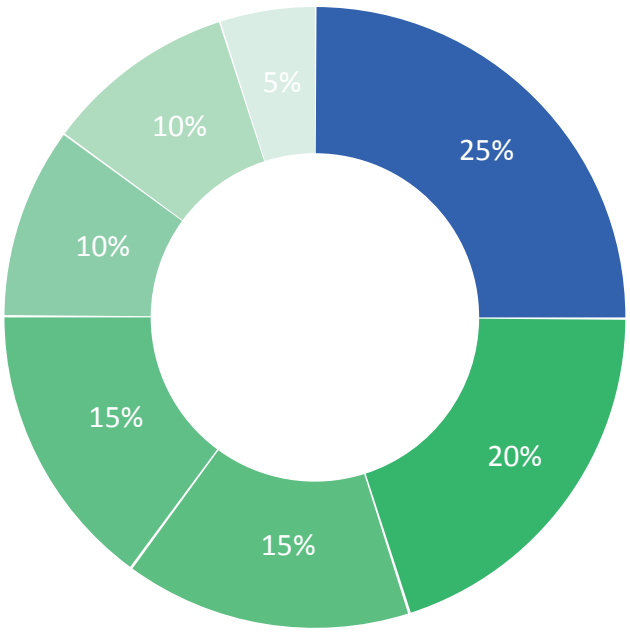
This white paper only introduces the token issuance plan of the XWS, and the plan of XBC will be revealed in the following white paper.

The establishment process of the X ecology is similar to that of the Space X rocket. It will undergo four stages, including ignition, first stage propulsion, second stage propulsion and cruise. The first three stages require fuel (funding) support, and the official will reserve 10 %+15%+20%, a total 45% of the tokens to help complete the fuel collection.

TOKEN ECONOMY

The total amount of XWS is 1 billion, and it will never be reopened. 100 million pieces are used for the fundraising of the ‘hope of the ignition’, and the exchange rate is 1 BCH = 30000 XWS. The subsequent two rounds of fundraising will be adjusted according to the valuation of the project to ensure that each XWS has the same eco-economic equity.

Before the hope ignition round, we will provide a donation round for a small number of angel investors. The donor's name and donation amount will be saved in the creation zone of the white X chain. For donors, we will perform random feedback based on the algorithm. The specific operation is that when the block height reaches certain random heights, all donors will be given a cash red envelope equivalent to the total transaction amount in the block according to the donation weight. The random seed is determined by the transaction hash and the number of transactions.



10% Hope ignition round

15% First stage propulsion round

20% Second stage propulsion round

25% Platform operation and ecological construction

15% XApp Eco-Incentive Pool

5% Black X chain block reward pool

10% Founding team and consultant

5.3 THE BUDGET OF RAISING FUNDS

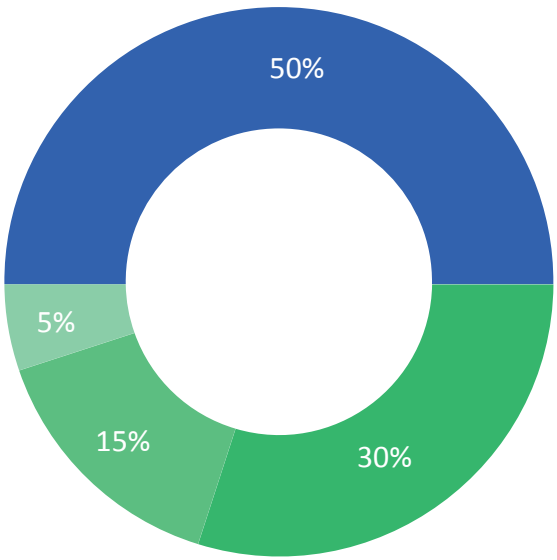
The funds raised by Project X in the early stage are managed by the Foundation for daily operations, technology research and development, business development and investment. The usages are classified as follows:

Technology development: this part of fund account for 50%. Expenditure on the technology development component includes the salary of the technical team, the recruitment fees of experts and developers, the cost of technical patents and intellectual property protection.

Business expansion: this part of fund account for 30%. Expenditure on funds in the business expansion segment mainly includes the cost of commercial promotion, technical exchange and sharing, supervision and compliance, alliance creation or participation in the Project X project.

Investment: this part of fund account for 15%. The expenditure of funds in the investment part mainly includes the Project X incubation project, the support or cooperation of other high-quality projects developed on the Project X double-stranded chain, and investment in other potential cryptocurrencies.

Daily operations: this part of fund account for 5%. The expenditure of the funds in the daily operation section mainly include the daily administrative and operational work of the Foundation, including office leasing, logistics management, transportation, finance and reporting.



50% Technology development

30% Business expansion

15% Investment

5% Daily operations

5.4 XWS APPLICATION SCENARIOS AND VALUES

The main purpose of the White X Chain is to quickly integrate high-quality project-side resources in the market through an efficient mechanism and generate substantial profit-sharing for all XWS investors through continuous tax hematopoietic capacity. XWS is a dedicated token for the white X chain ecosystem with multiple application scenarios and values.

5.4.1 *The elected representative node gets the block reward*

In the white X chain, as long as its position reaches the top 3000 of the whole network, it can be elected as the representative node, and the elected representative node has the opportunity to be randomly selected as the temporary committee member node to participate in the block production to obtain the block reward.

5.4.2 *Become a standing committee member and securely obtain block rewards and management rights*

The Standing Committee member nodes have great income and management rights in the white X chain, which is a reasonable mechanism to encourage large community positions. In addition to block rewards, the Standing Committee member nodes are also responsible for determining the daily affairs of the community. The daily affairs here refer to everything except the constitutional regulations. Changing the constitutional regulations requires more than 80% of the votes of all the representative nodes to vote.

5.4.3 *Act as developer's ecological access token*

The white X chain will open the API of the integrated project module. The developer needs to pledge and freeze a certain amount of XWS to the official before launching the project on the platform. This part of the token is will serve as loss compensation for the ecological user when the project party violates the community rules or goes offline. The official can not embezzle this part of token. It ensures the ecologically sound operation, and also promotes the circulation and scale application of the entire ecological token.

5.4.4 Obtaining project tax dividends on the white X chain ecology

The white X chain ecology has acquired a strong hematopoietic capacity while rapidly integrating high-quality project resources. Therefore, during the operation of the platform, it will continue to receive very rich tax revenues from the operation of the resident projects. In the white X chain economy, each XWS has the same dividend rights, and will not be differed due to node levels. So even if the position is not at the top of all the nodes, you can still enjoy the tax dividend that matches your position.

5.4.5 Enjoy the currency price bonus brought by the improvement of ecological valuation

The continuous growth of the white X chain economic and ecological cash flow will foster the continuous improvement of the entire ecological valuation. As the dedicated token of the white X chain ecology and the only equity dividend basis, the token price of XWS in the secondary market will inevitably increase as the valuation increase, which follows the same pattern as the equity of a listed company.

06
PROJECT ROADMAP

PROJECT ROADMAP

2020	Mainnet Online and Open Source
2019 . 10	XBC Listed on Exchange
2019 . 09	Black X Chain Fundraising
2019 . 06	XWS Listed on Exchange
2019 . 05	White X Chain Primary and Secondary Propulsion Rounds
2019 . 04	White X Chain, Ignition Round Fundraising
2019 . 03	Officially Releasing the Project White Paper
2019 . 02	Preliminary Completion of Technical Framework Cross-chain Communication
2018 . 10	Starting the Underlying Architecture Development
2018 . 07	Product Concept and Logic Initial Construction
2018 . 06	The Inspiration of Double-Dtranded Chain

07

RISK WARNING AND DISCLAIMER

RISK WARNING AND DISCLAIMER

XWS and XBC are Tokens that are one of Project X's usage scenarios. They are virtualized reward mechanism for system operation, not a monetary return. Therefore, redemption is not an investment. Holding XWS or XBC does not represent ownership of Project X or Project X applications. Project X does not grant any individual the right to participate, control, or make any decisions regarding Project X and Project X applications. Holders of XWS or XBC can participate in the usage of the Project X platform, but can not directly realize XWS or XBC. The value goal created by XWS or XBC is to create the application value of the application platform and usage scenarios, as well as the scarcity experience of virtual goods for participants and holders, rather than monetary value or transaction value. We cannot guarantee that XWS or XBC will add value, and it may also have a decline in psychological cognitive value under certain circumstances. The goals listed in this white paper may change in the light of unpredictable circumstances. While the team will do its best to achieve all of the objectives of this white paper, all individuals and groups that purchase XWS or XBC will do so at their own risk.

This white paper is only intended to convey the purpose of the information and does not constitute any investment advice, investment intention or investment in education. This white paper is not constituted and should not be interpreted as any purchase or sale, or any invitation to buy or sell, or any form of securities. Nor is it a contract or commitment of any kind.

Participants of Project X should carefully read the Project X white paper, fully understand the technical characteristics of Project X and the risk-return characteristics of the listing,. Participants should fully consider their risk tolerance, make rational judgment and prudent decisions. Once you participate in the project, you understand and accept the risk of the project, and you are willing to bear all the corresponding results or consequences.

08
REFERENCE

REFERENCE

[1] people on nxtforum.org (2014) DAG, a generalized blockchain //nxtforum.org/proof-of-stake-algorithm/dag-a-generalized-blockchain/(registration at nxtforum.org required)

[2] Sergio Demian Lerner (2015) DagCoin: a cryptocurrency without blocks. https://bitslog.wordpress.com/2015/09/11/dagcoin/

[3] Yonatan Sompolinsky, Aviv Zohar (2013) Accelerating Bitcoin's Transaction Processing. Fast Money Grows on Trees, Not Chains. https://eprint.iacr.org/2013/881.pdf

[4] Yoad Lewenberg, Yonatan Sompolinsky, Aviv Zohar (2015) Breaking free from chains: "Secure chainless" protocols for Bitcoin. https://dl.dropboxusercontent.com/u/7426164/Bitcoin/ Bitcoin meetup Chainless.pptx

[5] Sheldon M. Ross (2012) Introduction to Probability Models. 10th ed.

[6] Amir Dembo, Ofer Zeitouni (2010) Large Deviations Techniques and Applications. Springer.

[7] Sheldon M. Ross (2009) A First Course in Probability. 8th ed.

[8] Gilles Brassard, Peter Hyer, Alain Tapp (1998) Quantum cryptanalysis of hash and claw-free functions. Lecture Notes in Computer Science 1380, 163-169.

THANKS