ZORRO BLOCKCHAIN ZRO

FIGHT FOR——

JUSTICE AND FREEDOM!

WHITE PAPER V1.0

Directory

PREFACE

In 2020, the year of crisis, the world is in turmoil. The fire in Australia, the locust plague in East Africa and South Asia, the new global epidemic, the us stock market shutdown, the suspension of the Tokyo Olympic Games, the whole European Union "lock up", the foreign trade of the third world countries into trouble, let the already fragile economic situation, further worsen. "Stock god" buffett said that the economic crisis is not coming, but has already arrived; The only question is whether the economy will collapse as badly as it did in 1929.

In the face of the crisis, countries have to save themselves. The United States, Japan and Hong Kong have launched large-scale cash distribution programs to stimulate consumption, and the g20 online summit reached consensus on a $5 trillion economic stimulus plan. The Internet giants that used to fight collaboration, freedom, sharing and antitrust have become the new, bigger monopolists for their own business interests, monopolizing data that should belong to users themselves. And these data are closed in their own platform, forming a data island, and even use these data to manipulate and harm users, each service provider through the closed centralized account system, increase the difficulty and cost of user migration, users locked in their own platform.

Everyone aspires to a future that is smarter, fairer and more promising.

We hope that the segmented data can be broken down, rather than the data scattered in different places. There is a lot of redundancy and contradiction, which wastes a lot of resources but cannot form the overall resultant force.

We want people to be able to work with each other more trustfully, rather than against each other.

We want to have a decentralized trusted platform that provides safe and quality services to the world without having to spend a lot of time making comparisons.

We want the world to be more open and inclusive, so that every character can be treated equally, have a place in the world, and live with dignity.

We want future rules to be open and transparent, data and information to be more reliable, value to be more widely distributed, and credit to be more widely distributed.

Under the cover of the nest, there are no finished eggs. In the face of the disaster, the people who suffer the most are not the rich and powerful, not the rich and powerful businessmen, but the ordinary people. The collapse of the economy has led to widespread unemployment. It is hard for our generation to imagine what warren buffett meant by the "unprecedented year of 1929," but this could well be the toughest time yet.

The loss of wealth is only second, and the saddest part is that in order to get through these difficult times, we will have to carry heavy financial and even debt pressure for a long time to come, constantly running for food and clothing, no longer have any freedom to look at the poem and the distance.

What is freedom? Balzac said: "a thinking person is a man of real power." Rabindranath tagore traveled far and wide, tasted the world, and finally wrote in the immortal stray birds - crescent moon: "the bow whispers to the arrow before it shoots -- your freedom is my freedom." For he knows that if our efforts are not to fight for freedom, then all our efforts are but to strengthen the chains around our necks; Sadie also wrote in the rose garden that "even if the phoenix were to disappear from the world, people would not like to roost under the shadow of the owl." Any success that cannot be crowned by freedom is but a mirage. Thus, in "selected plays", stringberg throws up his arms and shouts: "it is the duty of a man to seek freedom in the light!"

We are just ordinary people, but we also have the desire not to be overwhelmed by the weight of meters, also have the pursuit of freedom belongs to our rehabilitation of human rights!

Unfortunately, although freedom is a natural right, its realization can not avoid the road of thorns and even "iron and blood", riskov wrote in the "father lobby", "freedom is not a gift, to strive for." In this struggle for freedom and the storm is about to sweep the crossroads, how we hope, can have a masked black man from the sky, the road to see the uneven bright sword to stand up, the evil police to punish the evil, the strong and the weak, to speed up the arrival of the great vision of freedom for all mankind.

"Xia is the greatest, the world is the greatest", Zorro public chain is inspired by the western legend of justice masked black man Zorro's brilliant imagination and precious spiritual inheritance, is committed to through the scale of justice, wealth and freedom of creation, all-round liberation of the user community and the soul of mankind.

"The fate of all is always dust," except for free souls.

ZORRO BLOCKCHAIN

1 INTRODUCE

IF A PERSON IS LOCKED TIGHTLY BY AN IRON CHAIN, WHAT USE IS THE WINGS FOR HIM? HE WILL ONLY FEEL MORE TERRIBLE DESPAIR.

—— [GERMANY] SHAMISO'S "STRANGE STORY OF PETER SCHLEMMER"

INTRODUCE

1. Overview of Zorro

Zorro deeply develops core technologies such as decentralization and distributed bookkeeping to realize a new electronic mutual trust system for global industry organizations, and first applies this system to global trade of physical goods, and gives priority to practice in international trade industry. Zorro will adhere to the principle of openness and win-win, build a digital currency payment system in the blockchain world, and promote the development of smart payment. Zorro will also build covers all kinds of the application of ecological public private chain chain and link each enterprise alliance, and use the Zorro Token (ZRO) through the alliance, the industry, the gap between each user, solve the problem of current payment industry many pain points, is the international latest top block chain architecture concept under the guidance of a global application scenarios and the grand blueprint of ideal block chain project.

Zorro hope, can pass to economic and social comprehensive digital chain, all things digital approval and the digital trade and investment and distributed storage based on block chain technology, information cannot be tampered with, such as excellent performance, implementation of all economic activity in the real fair, fair and open, put an end to any unreasonable exploitation and unreasonable deprivation of personal values, to build a new society there is no room for fraud, in which let all mankind can free unlimited wealth value, creative freedom and liberty and freedom of thought!

2. Zorro concept

2.1 link and drive the world with trust

No matter how the world evolves, the theme of "trust is just what is needed, consensus is the cornerstone, and cooperation is the driving force" will not change.

Zorro was born for the widest range of trust, consensus, and collaboration that can support a wide range of applications and applications

The block chain infrastructure of users, oriented to large-scale business applications, provides convenient, friendly, efficient and safe development and deployment environment, so that everything can be easily connected to the chain, creating a new distributed business ecology that links everything and collaborates with the world, and links and drives the world with trust.

2.2 construct intelligent evolutionary ecology

The development and evolution process of bitcoin let us see the underlying logic that a group of ordinary people can do an extraordinary career, and let us see the possibility that the foundation of an organization can last forever and transcend discontinuity. Zorro will explore ways to open up organizational boundaries, motivate and attract more and more members to participate in the process, and effectively collaborate and form synergy. To build a benign development of ecosystem, can forward iteration, self evolution, through continuous introduction of "negative entropy" break the second law of thermodynamics entropy die ", become a real decentralized intelligent evolutionary ecology, has strong anti vulnerability, in the process of continuous evolution, constantly broken cocoon into a butterfly, until forever.

3. Zorro design concept

By observing the development of cryptocurrencies over the past decade, we find that the idea of decentralization is not new. There is reason to believe that Zorro is capable of creating a complete ecology and a new dimension. We believe that Zorro not only carries a currency or an industry, but also brings true and comprehensive fairness, justice and openness to the world, enabling every participant to enjoy full freedom of privacy, wealth and ideas.

However, the realization of the above vision requires the common support of every Zorro user. Faith is priceless, but its appeal is not enough. We should not only create a fair and just environment, but also use iron facts to show the general public what absolute fairness and justice can bring to them. Therefore, in order to realize Zorro's vision, it is necessary to provide users with a sustainable and profitable mechanism so that they can spontaneously participate in the construction of Zorro's business network.

From the perspective of the basic logic of the financial market, Zorro believes that the price of any commodity is directly proportional to the cash flow into the market, but inversely proportional to the total number of available transactions in the market at that time. Therefore, as long as the fission cycle of the platform can be started, huge cash flow can be injected into the platform, and the scale of the platform can be expanded and the user can continue to benefit. At the same timeIn order to further enhance the participation of users, Zorro will set up a strict mechanism to give extra rewards to users who have made outstanding contributions to the development of the platform, especially the participants of the light node and super node, so as to fully demonstrate the fairness and justice of the platform.

As Zorro's value increases, a large number of users will participate in the expansion of Zorro's network. In order to promote the loyalty of users on the platform, but also in order not to waste of large users of natural reserves of great value, Zorro will further develop injection to center for social, to exchange center, to center city life function many applications such as plate, not only injected new energy to the platform, also bring great convenience for users.

With a combination of Zorro's revenue drive and a large number of users, the Zorro network will quickly spread across the globe, allowing the seeds of equity and justice to sprout in every corner of the world, providing the most powerful guarantee for realizing the grand vision of "bringing freedom to all."

Many a man has sacrificed his life and blood in the quest for freedom, but no one has ever achieved it. We are no greater than our forefathers, but the age has given us tools that our forefathers never had. Zorro will surely be the highest and the last milestone in the quest for freedom.

Because after this monument, no longer bound.

4. Zorro values

Justice, equality and freedom

ZORRO BLOCKCHAIN

2 TECHNICAL FRAMEWORK

> KEEPING SILENT ON THE JUST CAUSE IS A CRY FOR THE UNJUST CAUSE.
> --ARAB

Technical framework

1. Zorro model

In order to understand the essence of blockchain, first define the transaction-based blockchain model, quantify the parameters such as security, consistency, decentralization, and propose relevant functions to build a quantifiable blockchain model.

Block Ω chain system is composed of five parts, including: function f is consensus, V is a node set, T is the transaction data set, S is the message set, B is the set blocks. Block chain system refers to the system in which node set V writes the continuously generated transaction data set T into block set B and generates message set S through the consensus function f. The consensus function f, which includes the message consensus function fs and the block consensus function fb, is determined by the system. Node set V varies with time. T according to the current time, Vt said t moment system Ω node set, n - said t to t + 1 time in new system Ω node set, n - out said t to t + 1 moment exit system Ω nodes, then:

Transaction data set $T:=\{Tv|v\in\ v\}$ varies over time. For any $v\in Vt\cap Vt+1$, Ttv represents the unprocessed transaction set at time tv, Tt – inv represents the message set received at time t to time t+1, and Tt – outv represents the processed transaction set at time t to time t+1:

$Tt + 1\ v = Ttv + Tt - inv - Tt - outv$

The following is a theoretical perspective to explain the block chain, from the basic model to analyze, then talk about the construction of the system model, and then the design and implementation of the specific algorithm mechanism. It is hoped that the technical logic, development route, essence, advantages and disadvantages of blockchain can be described more clearly in a systematic, simple and complex wayZorroThe advancement of technology, the charm and infinite potential.

Message set S:={Sv|v∈ v} varies over time. For any v,u∈Vt∩Vt+1, Stv represents the message set at time tv, Stv,u represents the message set received from u from time t to time t+1, and St−out represents the message set that no longer affects the consensus function f after time t+1, then:

St + 1 v = Stv, Stv, u - St - outv + Ttv

Meanwhile, the message set Mt+1u,v=fs(Stv,Btv,u) sent from v to u at time t+1 is generated by the message consensus function.

Block set B:={Bv|v∈ v} varies over time. For any node v∈Vt∩Vt+1, Btv represents the block set confirmed at time tv, and Btv satisfies the chain structure. The block set of v at time t+1 when the block consensus function is generated is:

Bt + 1 v = fb (Stv, whether)

Message set S:={Sv|v∈ v} varies over time. For any v,u∈Vt∩Vt+1, Stv represents the message set at time tv, Stv,u represents the message set received from u from time t to time t+1, and St−out represents the message set that no longer affects the consensus function f after time t+1, then:

St + 1 v = Stv, Stv, u - St - outv + Ttv

Meanwhile, the message set Mt+1u,v=fs(Stv,Btv,u) sent from v to u at time t+1 is generated by the message consensus function.

Block set B:={Bv|v∈ v} varies over time. For any node v∈Vt∩Vt+1, Btv represents the block set confirmed at time tv, and Btv satisfies the chain structure. The block set of v at time t+1 when the block consensus function is generated is:

Bt + 1 v = fb (Stv, whether)

1.1 decentralization of consensus algorithms

The decentralization of blockchain system is reflected in many aspects, the key of which is the decentralization of consensus. Consensus decentralization is the most important difference between blockchain system and traditional Internet system, and it is also an important factor that determines the democratic security of blockchain.

Judging whether a consensus agreement is decentralised is a matter of opinion, and there is no widely accepted standard. The main purpose of decentralization is twofold: to decentralize the structure of the system so that it does not fail because a few nodes are disconnected, defected, or attacked; Consensus is achieved by the participants of the system, and this kind of democracy increases the transparency and credibility of the system and prevents the system from being controlled by oligarchs.

How much say each participant should have in the system requires consideration of two aspects: centralization and equity.

Block chain is a decentralized system, any node may become the stage center, but there is no mandatory central control function. First, the system needs to assign the weight wv to node v according to its computing power, system contribution or network transmission capacity. A fair and reasonable weight evaluation system can stimulate the operation of the system, improve the efficiency of cooperation, enhance the performance of the system and promote ecological development. For example, in the Proof of Work (PoW), wv is the proportion of power owned by v, and in the Proof of Stake (PoS), wv is the token proportion owned by v. We use:

W (U) : = wv

Represents the sum of weights of node set U in the system.

During the operation of a blockchain system, nodes in the system can profit from the process of packaging transactions, generating blocks, or other processes. The power av of node v in the system is defined as the expected profit ratio of v. In a completely decentralized system, each node of power and his weight is consistent, so the degree of centralized system Ω sigma can be defined as:

$$\sigma := \sum_{v \in V} |av - wv|$$

System Ω sigma value is lower, the higher the degree of decentralization system.

1.2 system security and consistency

Blockchain is a decentralized system without a central node to maintain block set B. The design of the consensus function f enables different nodes to maintain the same set of blocks, thus achieving consistency. However, there may be node v in the system, which does not follow the consensus function f and intentionally sends an error message Mt+1v to u, thereby affecting the consistency of other nodes' operation and the whole network. We call such a node a bad node. Bad node set:

Ht = v ∈ n | ∃ u ∈ Vts, t.M t + 1 v, u indicates the fs (Stv, whether, u)

If at any time t, meet W (Ht) or less eta · W (Vt), fault tolerance parameters are satisfied, we call system Ω eta, W here is the node weight function (see 4.4.1). Eta to the wrong parameters, we define the effective nodes at time t:

Ut eta = argmaxU ⊆ Vt | W (U) or greater (1 - (eta) W (Vt) {| studying v ∈ UBtv |}

And the system block set Bt eta = studying v ∈ Ut eta whether. If at any time t, arbitrary block b ∈ Bt eta is satisfied:

∀ k p t + tau Pr [b ∈ Bk eta] 1-2 - c or higher

We called tau Ω meet identify system parameter, c here is given a constant. Eta, given parameter definition tau (eta) for the system can meet the minimum confirm parameters. Consistency in the distributed system includes: the strong consistency (tau =

0), weak consistency (tau tau or less *), eventual consistency (tau (up). In the blockchain system, due to network delay and consensus, it is impossible to guarantee the strong consistency of the data of the whole network node at any time, so we can only go after the weak consistency. Given confirm parameters tau * , eta for a fault tolerance parameters,Confirm the parameters are satisfied, if the system Ω tau * , we call system Ω satisfy consistency. So that we can define the system safety Ω zeta for meet the confirmed parameters tau * eta, the biggest fault tolerance parameters:

Zeta = max0 eta 1 or less or less eta s.t. tau eta tau or less *

1.3 system performance

The performance of blockchain system is mainly reflected in the time required for the system to confirm the transaction, which is generally characterized by two parameters: the confirmation time (the time required when there is only one transaction) and the throughput (the maximum number of confirmed transactions per unit time). The confirmation time is the shortest period for users to conduct a transaction. If the confirmation time of a system is very long (for example, bitcoin takes about 1 hour), it will cause poor user experience and limit the application scenarios of the system. If the throughput is too small to handle all the transaction requests, some of the transactions are blocked or dropped, resulting in increased latency for the entire system.

More generally, given a transaction set T, d(T) is defined as the waiting time (delay) required for all transactions to be confirmed in T, and the expected value of that time is:

D (T) : = [D] (T)

Reflects the ability of the system to process transactions in T; The expected value here is to reflect the randomness of the system and the environment. When T contains only one transaction, D(T) is the confirmation time of the system. When T contains many transactions, D(T) can reflect the throughput of the system; Unlike a single metric like throughput, for a set of the same size, T, D(T) may vary (even dramatically) depending on the specific transactions contained in T.

A discussion of performance only makes sense if the system is sufficiently consistent and decentralized. , therefore, to improve the performance of the problem is that in the guarantee system of centralized degree of sigma sigma ＊ or less and a safety zeta zeta or ＊ under the premise of (sigma ＊ and zeta ＊ is the constant) system to optimize a function D. The definition here allows us to consider the transaction patterns in practical applications and to analyze and optimize them accordingly.

Confirming a transaction in a blockchain system requires consensus among all participants. In order to optimize the performance, the computational complexity and communication complexity of consensus algorithms should be improved.

The classic PoW consensus mechanism requires nodes to perform a lot of extra computation to gain the license of packaging, which greatly increases the computational complexity while ensuring the security and stability of the system. The subsequent PoS, DPoS, and some variants of them, avoided the additional expense of PoW, but the nodes still needed to be validated and signed, and the smart contract increased the amount of computation needed to process the transaction, and these calculations were unavoidable.

The communication complexity of consensus algorithms is divided into two parts: consensus participants need to reach a consensus first, and then broadcast to all nodes of the network. In order to achieve security under the premise of decentralization, that is, to allow a certain number of malicious nodes to exist in the network, a certain number of nodes must be verified before each transaction is confirmed, which requires all the consensus nodes to receive the transaction. Broadcasting can take place after a consensus has been reached without affecting the confirmation speed, but if there are many full nodes in the network, the bandwidth and time required for broadcasting may affect the performance of the network.

1.4 efficient consensus mechanism

For a transaction set T, the waiting time required for all transactions to be confirmed is:

DT = hdcompT dcommT, dempoT sigma sigma or less ＊ , zeta acuity zeta ＊

Calculation of delay, including dcomp said consensus dcomm said consensus communication delay, dempo said consensus permissions distribution delay, sigma, zeta decentralization degree and safety of the said system, sigma ＊ , zeta ＊ for system constant. In order to improve the efficiency of the consensus mechanism, it is necessary to optimize dcomp,dcomm and dempo in the performance function.

1、dempo

Dempo is mainly determined by the way in which the consent rights are allocated. In the existing blockchain system, the methods of distributing consensus permission mainly include PoW, PoS, DPoS, and identity authentication.

In the block chain system based on computing power distribution consensus permission, in order to ensure the degree of decentralization of the system, so that each node can obtain the influence av matching its right wv, the computing power proof function is required to make Gwork(wv)=av, at this time =0. But Gwork requires a lot of calculation, and dempo is high;

In the blockchain system based on the consensus permission of equity allocation, there is an easily calculated equity proof function Gstake that satisfies Gstake(wv)=av, where sigma =0 and dempo is low.

The blockchain system based on identity authentication and distribution of consensus permission needs to introduce third-party authentication to ensure the fairness and justice of influence distribution. This method is more suitable for blockchain of alliance chain type and not suitable for basic public chain.

2、dcomm

It is mainly determined by the size of consensus node set. If the consensus algorithm is unchanged, the smaller the set of nodes participating in the consensus, the lower the amount of data to be transmitted, and the lower the dcomm. The size of the consensus node set is limited by system security. Assuming system Ω node set V, safety coefficient of the Ω zeta, consensus is accomplished by a subsystem Ω c, Ω node set to U c, Ω safety coefficient for the zeta U c, the proportion of bad node z Ω c. The consensus subsystem Ω safety probability for c：

$$Pr(z\leqslant \zeta U)= \sum_{i\leq \Im u|U|} \zeta\ |V|i(1-\zeta)|V||U|-i|V||U|$$

When |, U, | is very small, although dcomm is very low, the security probability of the corresponding consensus system also becomes very low, and the reliability of the whole system decreases.

In order to ensure system safety meet the zeta acuity zeta ＊, consensus node set size should meet the | | U p ＊ k.

3、dcomp

Dcomp is mainly determined by the computational performance of the node. Under the condition that the consensus algorithm is unchanged, the higher the computational performance of the nodes participating in the consensus, the shorter the time required to complete the consensus, and the lower the dcomp. In the process of consensus, node v the computing performance of ev, influence of av node v, so the whole system Ω computing performance limit e Ω meet:

$$e\Omega \leqslant \sum_{v\in V} \partial v \bullet ev$$

It can be seen from this formula that the upper limit of the computational performance of the system can be increased by increasing the influence of node a or the computational performance of node e.Improve node performance: when the average computing performance of the nodes with influence of a in the system is improved by m times, the upper limit of the system's computing power is increased by ma times. Although the upper limit of the computational performance of the system can be raised by improving the computational performance of the influence nodes, due to the limitation of the Moore model, in a system with rapidly increasing performance demands, the performance of the entire system cannot be satisfied simply by improving the computational performance of the nodes.

Improve the node influence: in the traditional single chain system, v∈Vav=1, and through the multi-level hierarchical mode, m chain runs at the same time, can greatly increase the node influence. Suppose that the right of node v in the chain I isav,i， σ v∈V,i∈[k]av,i=m，So:

$$ev \leq \sum_{v\in v,i\in[k]} av,i\cdot ev$$

Even in a system with rapidly increasing performance requirements, it is still possible to increase the number of links to meet the performance requirements of the system and reduce the dcomp.

2、Trusted distributed computing platform (scalability)

From a system perspective, blockchain is a trusted distributed computing platform that can act as a Shared computing resource. Customers can view the platform as a next-generation computing facility. They send them any request. When the platform receives a request, it first checks its validity, then processes the request on some nodes and returns the result to the client. Through this process, data and messages are transferred over the platform, and compute nodes and resources are managed in a distributed manner.

In particular, an effective blockchain design should have the following attributes.

1. Safety

All the results are correct.

2. Liveness

Each valid request is processed in a fixed (small) amount of time. Here, we assume that the platform has a unified trusted interface that allows clients to send requests and receive results. In addition, consensus protocols are needed to ensure that the same content runs on different compute nodes.

The most relevant classic model is state machine replication. However, unlike the SMR model (which requires licensing [9]), the blockchain platform allows any node to join without permission. In permissionless Settings, nodes are not trusted, which introduces a challenging problem known as "witch attacks." In a witch attack, the attacker can generate a large number of compute nodes, most of which can then be easily controlled to reach a consensus. A common way to prevent witch attacks is to use a proof of workload (POW) [8] or a proof of entitlement (POS).

In our technology-related white paper, we describe the system model, conduct qualitative analysis from consistency, reliability, security, scalability and other aspects, and propose a framework for analyzing the scalability of blockchain system.

Throughput is an important system performance metric that represents the system's ability to handle requests. But that is not enough. When the system reaches its processing bottleneck, it must discard redundant requests from clients, reducing the availability of the system. Therefore, we need to have another performance indicators to assess the system limitation, Scalability (Scalability).

Blockchain scalability does more than show that system throughput can increase monotonously as the number of compute nodes in the system increases. In addition, scalability includes:

1. Load scalability, the ability of the system to adapt to heavier or lighter loads;

2. Function expansibility, enhance the capability of system functions by adding new functions;

3. The ability to update scalability by using a new generation of components.

We propose a framework for analyzing the scalability of blockchain systems, which are similar to distributed systems. Given the configuration C of the system, we use FC to evaluate the performance and cost of the system:

FC= F（T,S,Q）= T· Q/S

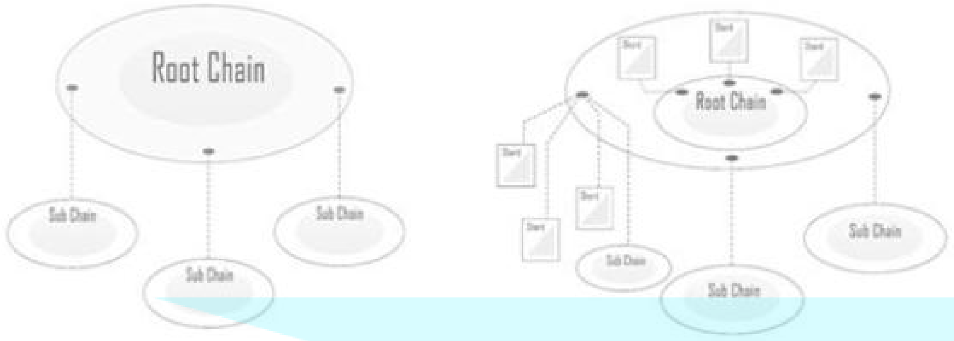
Where T and Q represent the throughput and service quality of the system respectively. S represents the total cost of the system, including node cost, network bandwidth cost, etc. For chain blocks, the Q is mainly composed of average confirmation time d and target time d decision. To normalize Q to (0,1) intervals, we setQ=$\frac{\mathrm{a}}{d+\wedge d^{\circ}}$And then as d goes to infinity, Q is equal to 0, and as d goes to 0, Q is equal to 1Given the initial configuration C, we can extend the system configuration to Ck by scaling factor k. Policy specifies how to expand the configuration. For example, when the initial configuration C has n nodes and policy increases the number of nodes by k, the number of nodes in the configuration Ck is equal to k • n. Then, we can calculate the scalability quantitatively:ψσ(k)=FCkFC

If the bits of sigma (k) is equal to 1 or increases monotonously with the increase of k, we say the system under the strategy of sigma with perfect extensibility.

3、Zorro architecture

3.1 multi-level chain structure

From an implementation point of view, our chain structure is a hierarchical chain structure.



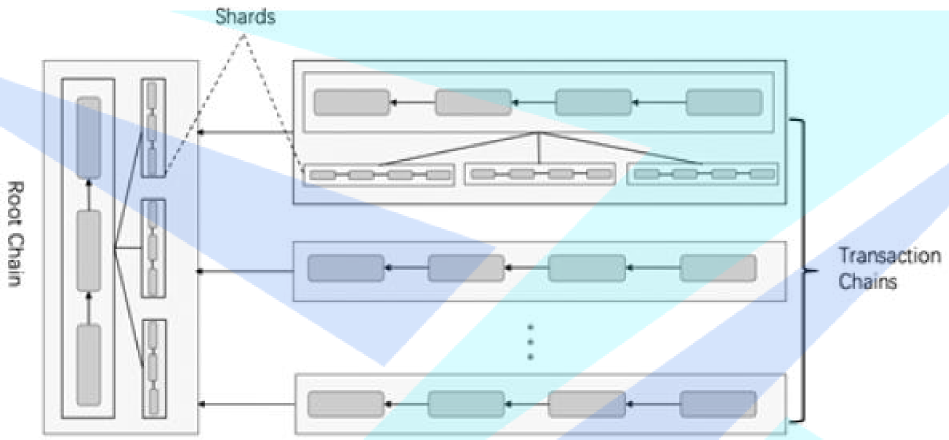
Zorro's chain is divided into two types: main chain and service chain. Each chain is a complete system with its own state. The main chain ACTS as the leader and coordinator of the whole system. It ACTS as the entry point and source of trust for the business chain, records the metadata and summary of each confirmed block of the business chain, generates random seeds used in the committee election of all the chains, and records the election results. At the same time, the workload from the business is Shared by all the business chains and contracts are computed in parallel using message-driven protocols based on the Actor model. All nodes in the system keep the state of the main chain. By updating and verifying the block of the main chain, the node can verify any block data of the business chain that has been included in the main chain. The structure has the following main advantages:

1. The node joining the system only needs to obtain the current state of the main chain from the trusted source, or rebuild from the creation block, and does not need to synchronize all the data of the whole system, which greatly reduces the load of the whole system.

2, the consensus of each chain is independent and parallel execution, greatly reducing the network bandwidth and computing processing requirements.

3. The main chain can act as the coordinator of the system, providing cross-chain synchronization and allowing the entire system topology to be dynamically adjusted.

4. A node can use the digest and Merkle proof in the main chain to verify transactions initiated from another business chain. Therefore, a block generator of a business chain does not need any information from other business chains to process inter-chain transactions.



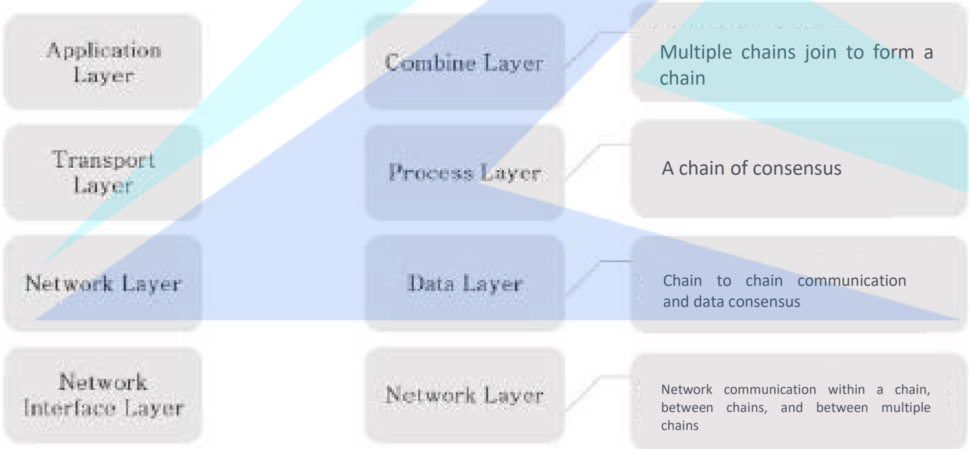
We can separate out different business chains to run separately according to different transaction types or business entities. They can be completely independent operation, cross-chain communication through the evidence provided by the main chain, also can be dependent on the dependent chain chain chain chain, where the child chain inherited part of the parent chain attributes, such as the account balance in the chain of the currency type, chain election method.

This relationship is logically related and has a direct impact on the chain's properties and network connections, making it easier to exchange data between sibling chains. Zorro's design principle is to allow each business chain to extend its own subchain downward, but in practice, problems can be solved up to three levels.

Both the main chain and the business chain can become congested due to too many requests. When congestion occurs, requests can be distributed to different shards by sharding the chain, so as to improve the throughput of the chain. As the number of shards increases, the throughput of the chain increases linearly. The shard itself is also a chain that runs independently, and there will be optimization of cross-shard transaction requests between the shards, which greatly improves the execution speed of cross-shard transaction between the shard chains.This hierarchical structure is flexible, scalable, and dynamically adjustable, so that each chain does not become a performance bottleneck for the entire network. Furthermore, as the number of chains increases, the throughput of the entire system increases linearly without generating too many redundant messages.

3.2 four-tier system structure

Based on the above layered multi-stage chain structure, we designed a four-layer implementation framework from the system perspective, in order to facilitate the future expansion and upgrading of the system.


Application Layer
Transport Layer
Network Layer
Network Interface Layer
Combine Layer
Process Layer
Data Layer
Network Layer
Multiple chains join to form a chain
A chain of consensus
Chain to chain communication and data consensus
Network communication within a chain, between chains, and between multiple chains

The first layer is the integration layer, which addresses the overall consensus of the system and is primarily responsible for dividing requests and nodes and assigning different requests to specific committees for processing. All requests are first sent to the integration layer, where they are split and assigned to different committees for parallel processing. Because not all requests can be processed in parallel, they need to be partitioned according to their type. In addition, all active nodes are registered at the integration layer. These nodes are randomly divided into different committees and assigned to different requests. We need to ensure that each committee is credible, that the percentage of malicious nodes within each committee does not exceed a certain threshold set by the system.

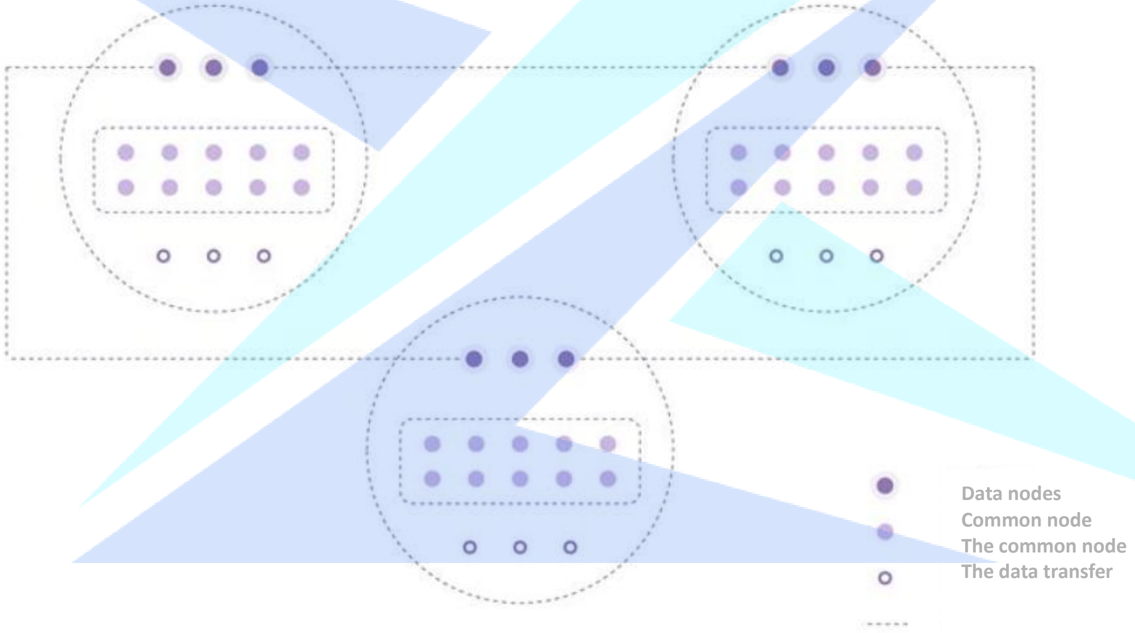
The second layer is the processing layer, which mainly solves the single-stranded consensus problem and needs to process the allocated requests and generate logs. Each committee contains a set of nodes, and when the committee receives a given request, it needs to process the request, reach a consensus, and generate a log. Since the credibility of each committee is guaranteed by the upper layer, the layer only needs to consider how to reach consensus in the committee as soon as possible.

The third layer is the data layer, which mainly addresses the consensus among multiple chains. The logs generated by each committee and the request data are aggregated according to specific coding methods to form a single log. The goal of the system is to generate consistent logs for each node. Therefore, an aggregation algorithm is needed to integrate all the logs generated by the nodes in the board and achieve uniform logging. You also need coding methods to reduce the storage per node. In addition, since nodes join and leave committees from time to time, the corresponding data from the data layer must be synchronized.

The fourth layer is the network layer, which mainly solves the communication between different attributes and task nodes. This layer is the foundation of the entire system, establishing communication between compute nodes. Within the network layer, we can build a multi-tier network, creating a consensus network layer for each committee.

4、Consensus agreement

In Zorro system, there are three types of nodes in each chain: data node, consensus node and common node. The data node is responsible for the storage of all the data in its chain and the interaction of information between chains. The main responsibility of the consensus node is the calculation, packaging and consensus of the chain, while the common node just carries the business. The diagram below shows the relationships between the different nodes of the chain.



The consensus nodes of each participant are randomly assigned, and they are constantly reselected as time changes.

4.1 committee selection

To resist witch attacks on unauthorized systems, we use an election algorithm based on share certificates (PoS).

Bitcoin, ethereum and other early blockchain projects use workload proof consensus (PoW). Consensus participants compete for bookkeeping rights through "mining," which involves performing certain complex calculations. Mining consumes a lot of power and computing time, but these resources do not contribute to the efficiency of the system. In fact, because confirming a transaction requires the reception and verification of most of the nodes in the network, the time required to broadcast information in the network increases with the number of nodes, and the efficiency decreases.

Furthermore, if consensus algorithms require each transaction to consume each participant's bandwidth, computation, and storage resources, the performance bottleneck of the system depends on the weakest participant in each dimension. In this case, to improve the performance of the system, only the nodes participating in the consensus are required to be "super nodes", which forms a DE facto centralization.

Therefore, we choose the consensus mechanism based on proof of interest (PoS). In PoS, the bookkeeping rights of a consensus participant depend on the assets it owns. In our consensus algorithm, consensus participants prove their interest by submitting a deposit. The system selects a certain number of participants according to the proportion of the deposit to form a committee to be responsible for the block for a period of time through the random algorithm.

Since only elected committee members are required to participate in each block, in a multi-chain system, the committees of each chain can exist simultaneously and operate independently of each other. As the number of nodes in the network increases, more subchains can be run simultaneously, thus making efficient use of the resources of nodes.

Compared with PoW, PoS consensus does not require mining, greatly reduces the threshold of participation and energy consumption, and is more likely to achieve true decentralization. On the other hand, unlike the fixed super node block of DPoS, the committee is selected by random election, which not only guarantees fairness, but also gives everyone the right to participate in the block and obtain rewards, and also prevents various problems that may arise from super node monopoly. Similar to PoW, the security of the PoS algorithm only requires the assumption that most of the benefits do not belong to malicious attackers and that the network satisfies weak synchronization.

The selection algorithm requires the following security properties.

Assuming that the honest node's share ratio among all participants is 0, at least 1 of the committee members elected in each election is honest. Moreover, the algorithm should be fair, since the probability of each participant being selected is (roughly) proportional to the number of shares the participant has invested.

Committee members should be fluid and unpredictable so that opponents cannot attack the system by corrupting committee members (assuming that corruption outlasts the life of the committee).

In Zorro, we implement the above attributes through the following procedure. First, before the election, because all nodes only listen to the main chain, the subchain must signal on the main chain when the next committee needs to be selected. All chain elections are carried out on the main chain. Through the summary information on the main chain, the main chain can collect the election status of each chain for summary release. At the same time, the main chain will generate random seeds periodically to ensure the randomness of the selection of each chain.

Nodes willing to participate in the consensus need to register on the main chain by sending a special type of transaction. The deal also specifies the amount of equity that will be transferred to a specific share account and frozen until the node exits and the stake is withdrawn.

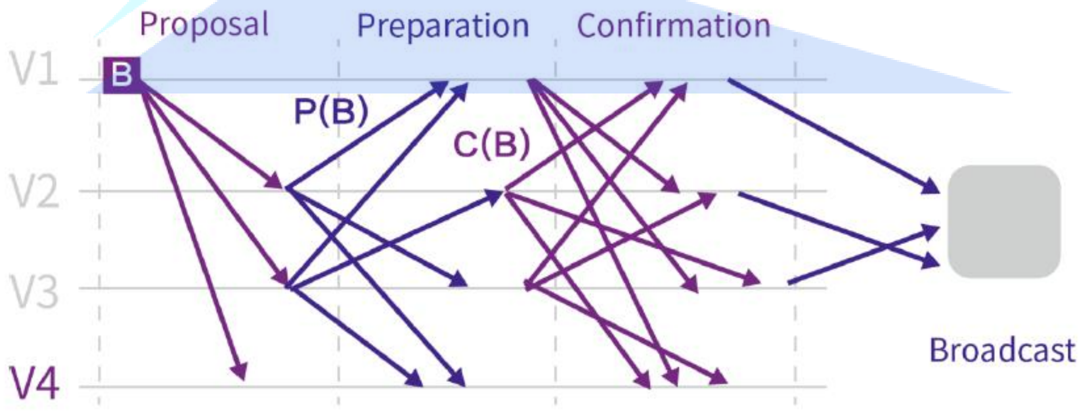
After the main chain publishes the election information, the consensus participants can see the election information on the main chain, calculate the value of a verifiable random function using the corresponding random seed and their own private key, and decide whether they are selected or not. When a node finds that it has the right to join a chain committee, it will first join the network of that chain and send its ID and verifiable random function proof, which will be recorded by the current committee. At the same time, new members of the committee need to prepare for consensus participation by joining the committee's network. They also begin to chain with the same steps. The received blocks and states can be verified using a digest on the main chain.

The elected nodes will establish a small consensus network for communication within the committee. Having a dedicated network reduces latency and bandwidth consumption for point-to-point communication and broadcasting between committee members. On the other hand, if not set up properly, the network may be less stable and more vulnerable to attacks. You need to ensure that the network topology is robust and that node information is securely exchanged using encryption. By the beginning of the next era, the new committee should have generated new keys, synchronized and updated the current state of the chain, and established connections in the new consensus network.The fairness of the election is crucial to the security of the system: if an attacker can hold a majority of seats on a committee, that committee cannot get out of the way. On the one hand, to ensure that random seeds cannot be manipulated, each random seed is generated by a group of members of the committee using a threshold signature: this makes it much harder for an attacker to predict which random seeds will follow and to prevent random seed generation, rather than being generated by the blocker alone. On the other hand, we have designed incentives so that honest commission members will be willing to record new commission members, rather than seek to retain their right to vote by sabotaging elections.

4.2 consensus of the committee

We assume that there is a partial synchronous communication model within the commission, in which there is an effective Byzantine fault-tolerant algorithm, and a customized PBFT variant is designed for this purpose. Committees account for only a small fraction of the network's nodes, and they themselves build a smaller network to reduce broadcast delays, thus steadily and efficiently outputting them. Due to the nature of the PBFT algorithm, when the nodes in the committee satisfy the weak synchronization hypothesis, the block-out algorithm can be safely run without more than half of the malicious nodes. Therefore, on the premise of the security of the election algorithm, the activity, correctness and uniqueness of each committee block can be guaranteed. In addition, our deposit and penalty mechanisms make it costly for committee members to do evil, thus encouraging honest users not to do evil and to report others' malicious behavior.

The execution of a node can be divided by wheels. Each round consists of three stages: proposal, preparation and confirmation.



The execution of a node can be divided by wheels. Each round consists of three phases: proposal, preparation, and confirmation (as shown above). State transitions are event-driven. To keep the system active in the event of a network failure or malicious attack, local clocks may trigger timeouts.

1. Proposal stage: the person in charge of the committee broadcasts the proposed proposal to other committee members.

2. Preparation: after each committee member receives the proposed block, a message containing the block's signature is broadcast. If a timeout is triggered before the proposed block is received, the committee member signs and broadcasts a special message to the other committee members (indicating that the leader is defective).

3. Confirmation phase: at the end of the preparatory phase, each committee member signs and broadcasts a copy of the signature received during the preparatory phase. Signature aggregation can be used to significantly reduce the message size in the validation phase.

Based on the information received during the confirmation phase, each committee member may decide whether an agreement has been reached on the block and broadcast the agreed block or blank block and evidence of its decision.

Malicious node punishment. In the case of a node that is clearly misbehaving (for example, a node that sends different messages to different nodes at the same stage), the round is aborted by outputing an empty block. However, the economic penalties for misbehaving nodes make such attacks unsustainable.

If the number of signatures received during the preparation phase means that most honest committee members have received the same proposed block, committee members may reach an "early consensus" that members can use the signature to print the block as proof of agreement (a different form than a regular agreement) before the confirmation phase. Note that the node still needs to participate in the validation phase.

4.3 Safety analysis

Let N be the number of nodes, N be the number of nodes expected in the committee, and m be the number of committees. The number of malicious nodes is lambda N. When the node in the committee that exceeds the ratio is a malicious node, we say the committee election has failed. Without loss of generality, we set N= N dot m. Suppose there is a completely random oracle O:[N]→[m]. Fix a committee that defines the percentage of I > events in which the Ai becomes a malicious node in the committee. So for each I ∈[m], we have

$$\Pr[Ai] = \sum_{\chi=\rho n+1}^{n} \frac{\binom{\lambda N}{x} \bullet \binom{(1-\lambda)N}{n-x}}{\binom{N}{n}}$$

With union bound, we get

Pr∪i∈[m]Ai⩽m· PrAi

By setting the appropriate parameter Settings, we can ensure that the probability of the event is negligible.

5、Multi-chain parallel model

For multi-chain systems, the account model for the current single-chain system (for example, UTXO or ethane accounts) no longer fits the new requirements, especially when dealing with a large number of cross-chain operations. We designed a new account model that allows us to implement complex logic on multi-chain systems in an asynchronous and lock-free manner. In this model, we separate transactions involving a set of accounts into multiple steps in the form of a message. Each message is received by a unique principal and executed by the corresponding chain. Finally, all messages are executed to achieve the transaction.

5.1 general parallel model

There are many mechanisms in parallel computing, including single-machine local computing, distributed network computing, such as locking, etc., but these are poor or not applicable to block chain multi-chain parallelism. We delve into the Actor model, proposed by Hewitt et al. [3] in 1973, which is a conceptual model for dealing with concurrent computing. It combines many scenarios to design new parallel applications, such as partial E-mail systems, Web services, and objects with locks in Java.

An Actor is a basic cell of computation. It can receive a message and perform calculations based on it. Its important feature is that the actors are isolated from each other, they do not share memory with each other, each maintains a private state, and this state cannot be changed by the other.

When receiving a message, the cell can simultaneously:

1. Send a limited number of messages to other cells;

2、Create a limited number of new cells;

3. Specify the behavior to use when the next message is received.

The above actions have no assumed order and can be executed in parallel. Each cell can receive messages from other cells. Messages are sent asynchronously to the cell, and each cell processes the messages sequentially, with no restrictions on the order in which they arrive. Multiple actors can run at the same time.

5.2 Zorro parallel model

We designed an actor-based parallel model as our basic framework. In Zorro, the structure mainly contains the following information:

1. Address: the unique identification word of the blockchain account.

2. Balance: the current balance of the account.

3. Nonce: scalar value equal to the number of external messages sent from the address.

4. Code: the programming logic for handling messages.

5, storage: the internal state of the account, can be empty.

Each account is controlled by a private key. In the code, the account defines its own processing for the messages it receives, allowing it to send messages to other accounts, create new accounts, and modify internal state. For some of the canonical messages, each account has the same general handling (such as "tran" and "add"). Each account can also customize methods for other messages.

There are two types of messages: external messages and relay messages. The external message is created by the account that signs it with the private key. The relay message is generated by the account that executes the send command during execution, which is somewhat similar to the message in ethereum. The big difference is that relay message execution is asynchronous in our model and synchronous in ethereum. Therefore, these messages in our model support cross-chain propagation.

The messages in Zorro mainly contain the following information:

1. Sender: address of message sender.

2. Recipient: address of message receiver.

3. Nonce: scalar value is equal to the number of external messages sent by the sender, which is null for relay messages.

4. Input: specify the input data group for the message invocation.

5, verify data: identify the sender of the signature of the external message, or relay message proof.

For external messages, you can validate with signatures and nonce. For relayed messages, it can be verified by proof.

5.3 block chain calculation based on parallel model

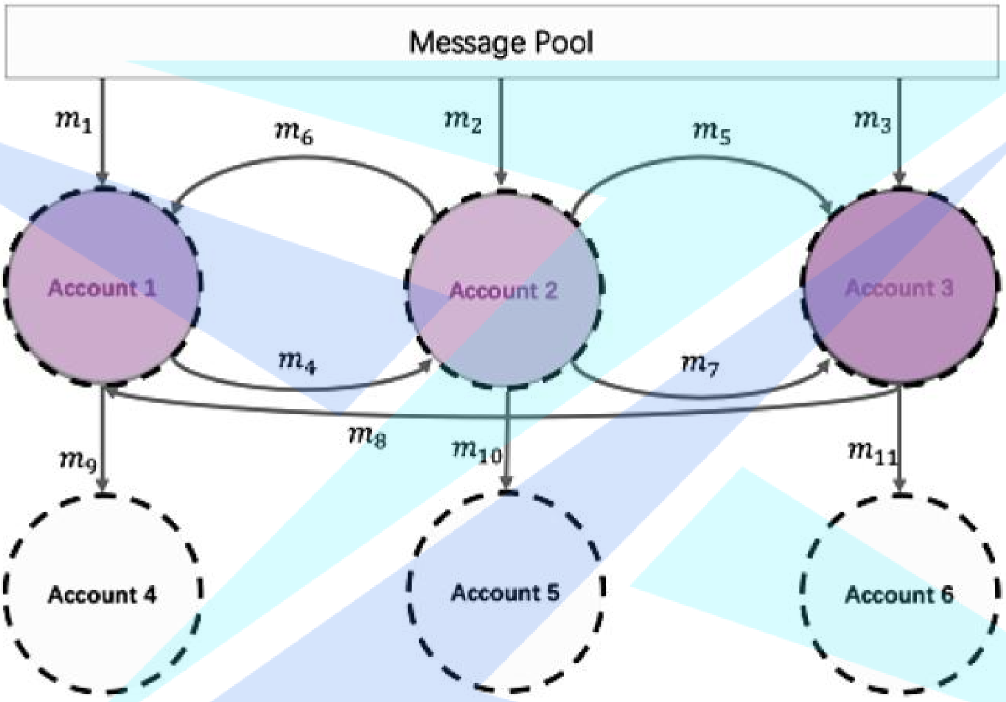
In our parallel model, there are three types of messages for each block on chain C:

1. Enter a message. These messages are not currently acknowledged, and the receiver account is on chain C, which can be external messages or relay messages generated by other chains.

2. Internal relay messages. These are the relay messages generated during the

execution of the entire block, and the receiver is also on chain C, so they are recognized on this block.

3. External relay messages. These are the relay messages that are generated during the execution of the entire block, and their receivers are on other chains, and these messages will be validated by other chains.



Here is an example shown in the figure above. There are three accounts 1,2,3 on the C chain, and three accounts 4,5,6 on the other chain. In particular, there are three input messages (i.e. M1,m2,m3) that are received by accounts 1,2, and 3, respectively.

For each account I, we use I to indicate the order in which messages are processed and the generation of new messages. Then we have:

σ 1=m1:m4m8m6:m9

σ 2=m2:m5,m6m4:m7,m10)

σ 3=m5:m11m3:m8m7

Thus, 1 means that account 1 processes messages m1, m8, and m6 in order. The internal relay message m4 is generated by processing m1, and the external relay message m9 is generated by processing m6. Then we have the internal relay message set m4,m5... ,m8 and external relay message set {m9,m10,m11}.

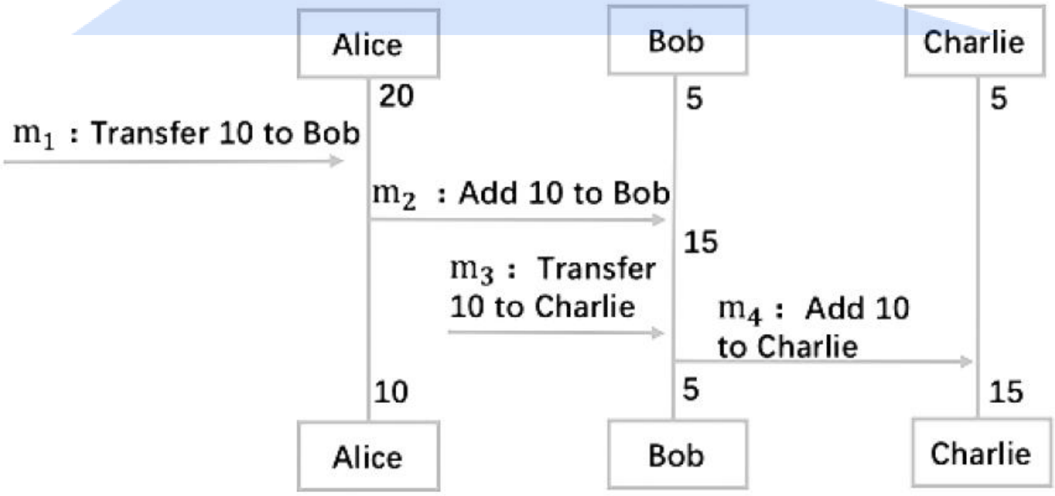
Upon receipt of the block proposed by the responsible person, members of the committee need to verify that there is no malicious responsible person. In our system, the node validates three parts:

1. Validity of each input message, that is, {m1,m2,m3}.

2. The processing period of each account is {1, 2, 3}. They can be verified independently and in parallel.

3, the effectiveness of processing message order, that is, order =(1, 2, 3).

To verify processing message order, we establish a directed graph G. For the two events e1 and e2, e1→e2 means that the occurrence time of e1 is before the occurrence time of e2. Set mi to indicate that the event account I received the message mi, and mi to indicate that the event account I sent the message mi. And then we have mi→mi for each I, for example I =1, we have m1→m8→m6. Based on these relations of, we can establish a directed graph G.


Alice
Bob
Charlie
20
5
5
m_1 : Transfer 10 to Bob
m_2 : Add 10 to Bob
15
m_3 : Transfer 10 to Charlie
m_4 : Add 10 to Charlie
10
5
15
Alice
Bob
Charlie

Theorem: processing message order =(1, 2, 3) is valid if and only if the directed graph G does not have a ring.

2.5.4 optimization

We designed some optimization methods to reduce communication costs and account storage.

Avoid duplicate storage. Each account has the same general handling for certain messages. These public methods are designed by the system and do not need to be designed by each account.

2. Reduce communication cost. Communication costs can be reduced by merging a bunch of messages of the same type. For example, if you have 10 "add" messages sent to the same account, you can combine them into one "add" message.

For the "single account hotspot" problem, where a single account involves a large number of messages, this can be easily resolved through the collaborative design of the upper application, similar to the "hot cat" problem, where many frequently used accounts can be placed on multiple chains.

Our model is more flexible and efficient than other methods that are also used to do concurrency. However, when developing with this model, developers need to be clear about the scale of cross-chain communication, otherwise multiple cross-chain interactions are likely to offset the efficiency generated by parallelism.

3

VALUE

> THE SAME SUN IS SHINING ON HIS PALACE, AND HE HAS NOT AVOIDED OUR HUT:
> THE SUN IS TREATED EQUALLY.
>
> -SHAKESPEARE

ZORRO BLOCKCHAIN

THE VALUE OF ZRO

1. Zorro's advantages

Zorro essentially USES blockchain technology to try to solve various pain points in the industry and build a "global blockchain free trade zone". In the free trade zone, Zorro provides the underlying block chain infrastructure, and introduces Zorro's Token system as the measurement standard for value transmission of trade activities between small and medium-sized merchants. In various application scenarios, Zorro will work with many third-party service organizations around the world to build a platform integrating e-commerce + payment, e-commerce + supply chain traceability, e-commerce + supply chain finance, e-commerce + community live broadcasting, e-commerce data + digital currency exchange.

Zorro, hope to be able to use digital thoughts, do not tamper with the system of distributed timestamp and ubiquitous, all things on the Internet, instant chain business system, properly completed these ambitious goals, truly a complete coverage of comprehensive, fair, just, for "free" mankind's highest goal to provide strong support.

Zorro will implement this step by step and provide services such as prompt payment, quick payment, cross-border payment, global legal currency and information tracing for the existing pain points in the aforementioned e-commerce market. More services can be extended in the future, including a local incubation service and a service to issue culture tokens on Zorro.

Zorro's design takes full account of openness and compliance and will comply with local regulatory requirements and regulations. Due to the openness of the Zorro blockchain, the regulator can set up nodes on it if necessary, or provide transaction records through Zorro. Due to the non-tampering nature of blockchain, this move will fully help the supervision to improve its supervision accuracy when necessary.

2. Development of Zorro

Along with the growth of world economy and a fair and justice, freedom and equality concepts is deeply rooted in the hearts of the people, Zorro will have great potential for the circulation at the same time, and there is a clear limit because the quantity of Zorro, without the risk of random spam, so Zorro will obtain more and more people with their stable circulation, to the holders of the sustainability of the big benefits.

Zorro's positioning is to deeply develop the block chain technology, develop the service network based on the platform's huge and outstanding comprehensive ecological functions, and build a comprehensive economic platform in the block chain world, so as to provide rapid, confidential and secure transaction services for the world economy and trade and even the entire payment environment.

Zorro is acutely aware that the essence of money is trust and circulation, and that trust must be Shared by all those involved in the circulation, rather than being left to traditional centralised institutions. The key to circulation is freedom, not excessive regulation. And this is what Zorro hopes to provide for society.

In the early stage of Zorro's development, Zorro will be mainly used to purchase various services of the platform. With the gradual emergence of Zorro's market capability, the circulation scope will spread to Zorro's cooperation units and even the whole online transaction, and eventually become the most important payment means for online transactions in the world.

3. Zorro's original intention

Imagine trading with strangers without trusting them; You don't have to trust the bank to keep your savings there. You don't need to trust any merchant, broker or broker because you know it has to be fair and just. What's going to happen?

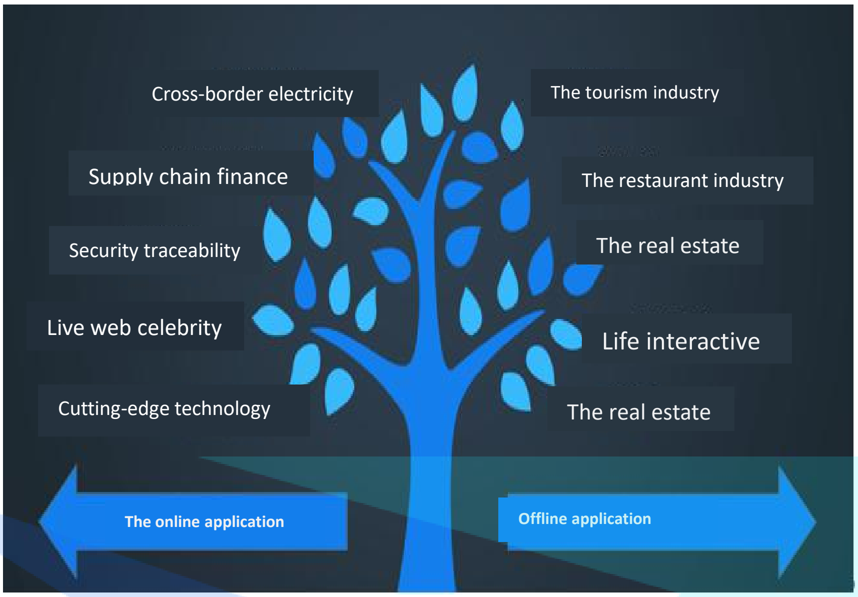
That will change the world.

And that's the vision of blockchain. While the mainstream media has been busy speculating about cryptocurrency prices and their black-market schemes, they have missed the essence of all this. Cryptographers have quietly invented a whole new set of prototypes. Blockchains (and the consensus protocols that support them) were born as developers tried to solve a bold conundrum: how to create digital currencies that cannot be traced back. By combining cryptography, game theory, economics and computer science, they have succeeded in creating a whole new set of tools for building decentralized systems.

Blockchain is not far away, it has come within reach of the eyes, it is a part of the Internet, in the transportation, medical, clothing industry, property rights, payment, life services and other fields have appeared many application scenarios, blockchain let the Internet wave upgrade again, and gradually into more innovative areas. In digital money. Blockchain is not only a technological innovation, but also reveals the possibility of building a new economic model by the decentralized and trustless thinking behind it. In the field of value empowerment and transfer, blockchain technology has begun to show great advantages due to its open, transparent, traceable and untamable characteristics. Eventually, it will help us complete the value migration of asset digitization and achieve real control over our own wealth.Unfortunately, the emergence of new technologies has always been shunned by vested interests for upending the structure of the economy. And this kind of boycott to the rapid marketization of emerging technologies, the practical process of the obstacles are multiplied. Up to now, the blockchain technology market has been overly concerned with the issue of new digital currency, the operation of the digital currency market is chaotic, and many other chaotic situations, which pose a serious threat to the economic interests of the majority of investors, thus greatly hitting the entry willingness of a large number of potential investors. And in a third world country markets, because of its unique financial regulatory system, chain blocks the development of technology is more difficult, such as the market standard, standardized process, such as high quality exchange market efficiency improve of the construction of the necessary elements is impossible, make block chain markets around the world so far is still in the "ghost" of the state to be developed.

And Zorro project purpose is, in this complicated era, in this block chain, purpose and the significance of the prospects are greatly distorted, carrying the banner of "fair, universal freedom" implementation to bring back block chain technology to the power to change the world, and restore the cutting-edge technology were dusty already a long time of the original face, back to the benefit of all mankind, and promoting social justice, the pursuit of humanity freedom career on track.

4、Zorro scalability



Cross-border electricity

Supply chain finance

Security traceability

Live web celebrity

Cutting-edge technology

The tourism industry

The restaurant industry

The real estate

Life interactive

The real estate

The online application

Offline application

4

THE CORE

> THE TRUE VALUE OF A PERSON FIRST DEPENDS ON HOW MUCH AND IN WHAT SENSE HE IS LIBERATED FROM SELF.
>
> -EINSTEIN

ZORRO BLOCKCHAIN

THE CORE

1. Blockchain infrastructure

The decentralized and self-governance system represented by block chain technology is attracting more and more attention and research. Currently, there are more than 20,000 blockchain projects in the world, and the total value of global encrypted digital assets reaches 200 billion us dollars. The user population in blockchain/digital assets is also growing rapidly. From 2 million users worldwide in early 2013 to 75 million in early 2019. We believe that the global blockchain/digital asset users will reach or exceed 200 million around 2020. It is expected to reach 1 billion users around 2025.

With the popularization of blockchain technology, more and more application scenarios of blockchain technology are discovered. The application scenarios of blockchain technology have gradually expanded from the original digital currency itself to more scenarios and user groups. For example, communities represented by ethereum introduced the concept of smart contracts in blockchain technology, while Ripple implemented a global settlement system using blockchain technology. With the diversification of application scenarios, users' demands for blockchain technology are increasing day by day. We have seen many challenges:

1. Lack of value scale

Block chain, we think, the world needs — a universal value measurement, to measure the value of user and intelligent contracts, upper application can be on the value of the universal scale combined with their own scene dig deeper value, which will bring more business model innovation, as the rise of Google in the interconnected world sample.

2. Establishment of block chain application ecological environment

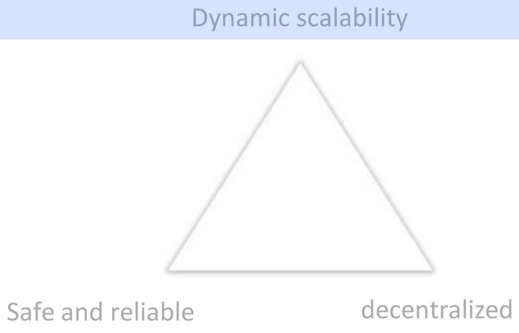
With the rapid growth of various applications (dapps) on blockchain, a good ecological environment is the fundamental to improve user experience. This includes how the user retrieval in mass block chain application expectation DApp, how to motivate the development 人 member to provide users with more DApp, and how to help develop faster build better DApp 人 member. Etheric fang, for example, based on the etheric lane on the number of total DApp has 十 wan, imagine if block chain DApp close to apple AppStore application total scale of the world, how to find and locate the desired DApp is a 大 problem.

3. Lack of innovation

"Blockchain for the sake of blockchain" is a very common phenomenon in the current field of science and technology, because the three words "blockchain" not only brings its own traffic, but also brings its "enigmatic" attribute. Such as Ankr block chain that paragraph of time very hot cloud computing platform, known as the use of independent research and development PoUW technology new technology of cloud computing services based on block chain and workload calculation mode, but the personage inside course of study in-depth analysis of its working mode, found Ankr compared to the previously seen multiple cloud computing platform also failed to block chain is used to calculate the real realization of cloud computing platform operation logic and the breakthrough of business model. The so-called "self-developed PoUW pattern" is nothing more than the use of Intel's SGX processor encryption technology for information upload, and SGX technology itself can fully realize a series of platform advantages claimed by Ankr, such as real workload statistics, workload and quality cannot be false, and distribution according to work. The proliferation of these "pseudo-blockchain" has made many consumers and investors who are interested in blockchain technology gradually stand in awe of the three words "blockchain".

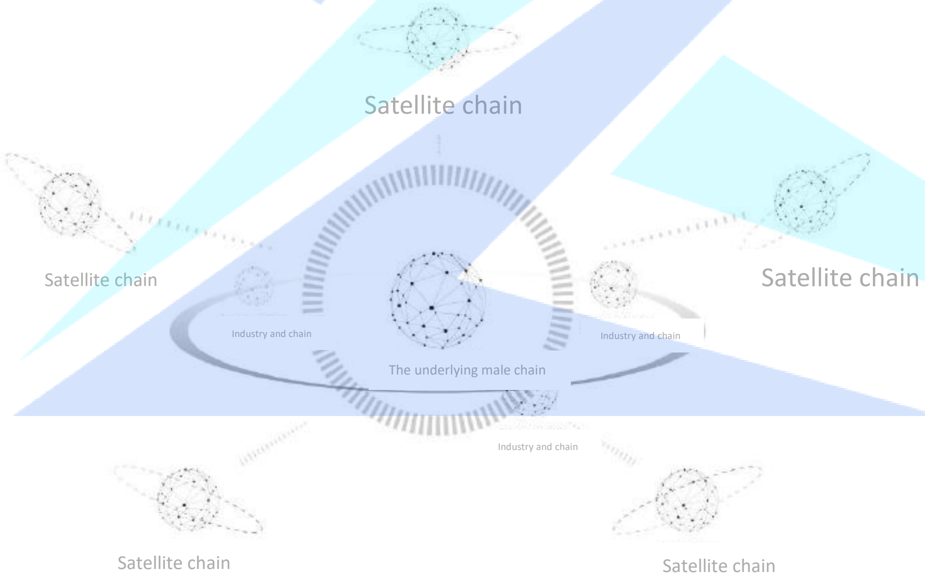
With an open, inclusive and mutually beneficial attitude, Zorro gives developers the world's leading three technological innovation advantages of public chain, alliance chain and privacy protection, so that developers can develop their own industrial public chain, alliance chain or application based on Zorro's bottom layer instead of being restricted by technology, so as to find their original intention and meet their dreams.

2. Commercialization

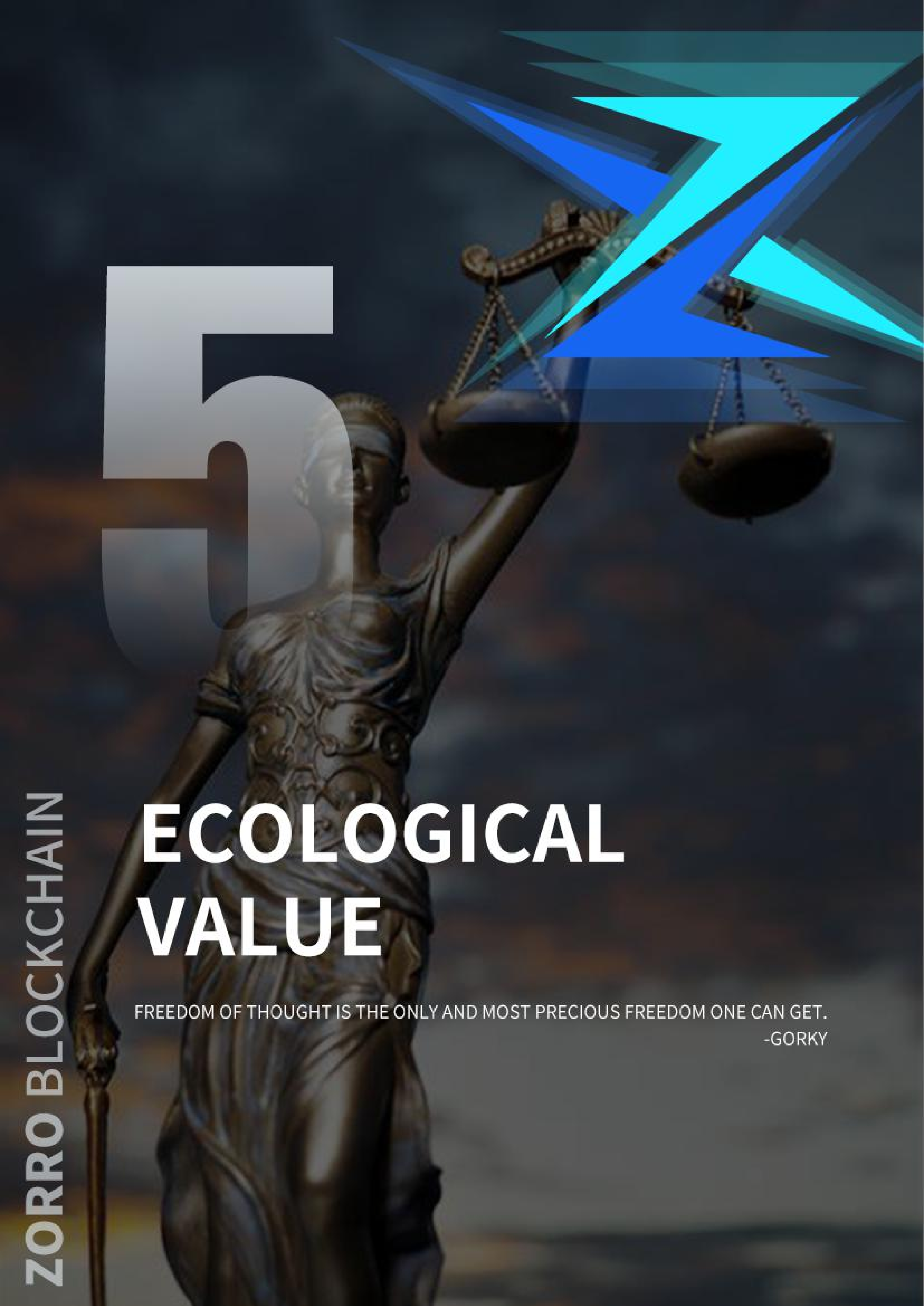


Zorro supports horizontal and vertical bidirectional dynamic expansion under the condition of ensuring the security and consistency of the entire system through the layered and multi-level architecture and the independently developed layered consensus protocol stack technology, thus fundamentally solving the "impossible triangle" problem of blockchain. On the basis of solving the problem of impossible triangle, Zorro also innovative put forward based on the Actor model account system, the perfect support for complex tasks of high concurrent processing, let the chain block capable of carrying more efficient large-scale trading, capable of supporting the application to run up huge amounts of user size, make originally because of limited by technology maturity block chain business project possible landing.

3. Value network



Zorro's entire value network can be understood to consist of Zorro's underlying public chain + extensible satellite chain. Zorro can build industrial public chain on the bottom of the public chain, the satellite chain is the alliance chain. If it is industrial common chain, its underlying security is consistent with Zorro's underlying common chain and other industrial common chains, and the value can be directly transferred; If it is an alliance chain, the underlying security is inconsistent, and the value transfer process requires additional protocol guarantees. Developers can develop DAPP directly on Zorro's underlying public link or on the industry public link, as well as capture part of the value of the satellite link already linked to Zorro. Developers can also develop DAPP on the satellite chain, which can deliver some of the value between different satellite chains through Zorro.



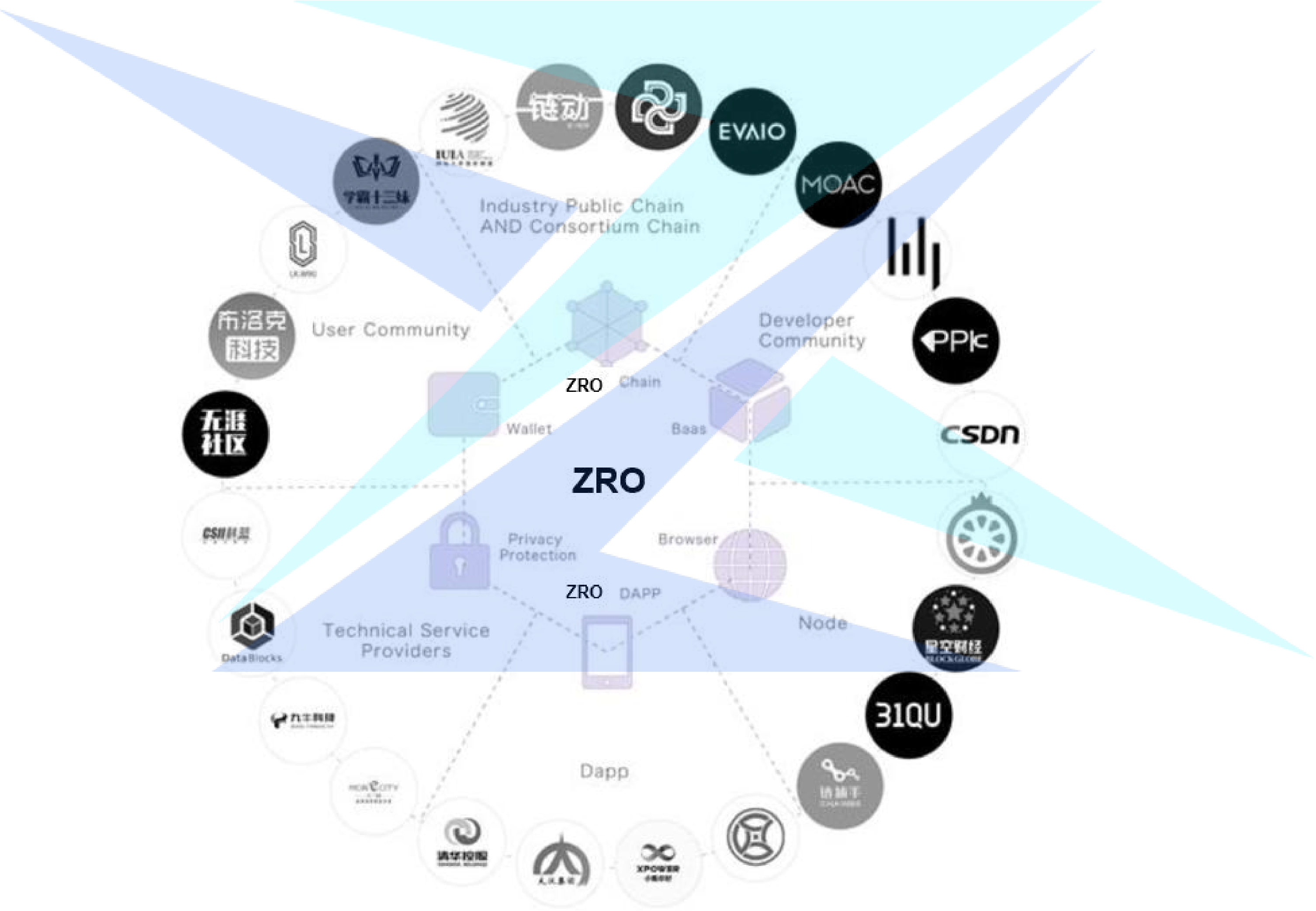
ZORRO BLOCKCHAIN

5 ECOLOGICAL VALUE

FREEDOM OF THOUGHT IS THE ONLY AND MOST PRECIOUS FREEDOM ONE CAN GET.
-GORKY

ECOLOGICAL MODEL

1. Zorro ecosphere

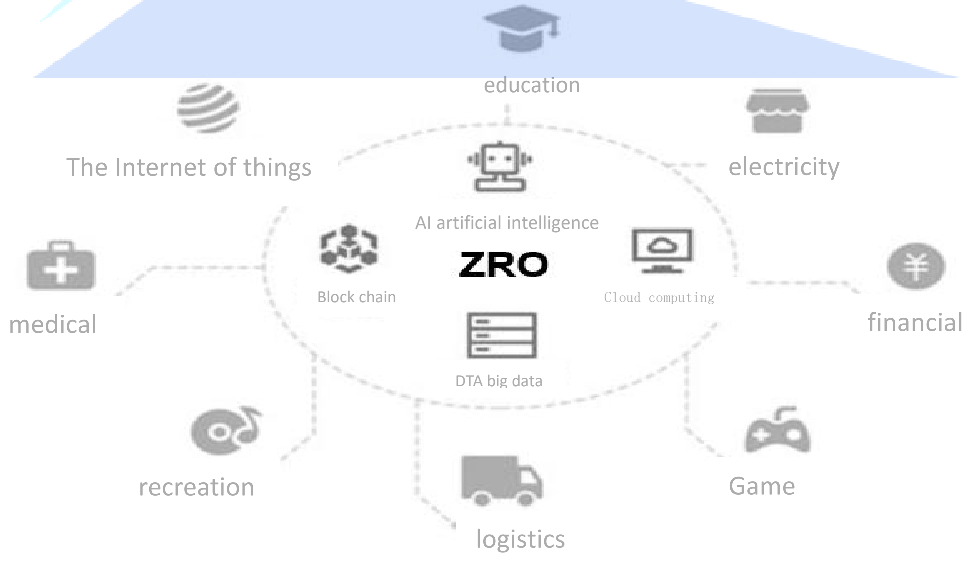


Zorro business ecosystem includes Zorro public chain, alliance chain, privacy protection and block chain applications such as DAPP, wallet and browser. Meanwhile, it provides convenient, friendly, efficient and safe development, testing, deployment and operation environment for large-scale commercial applications such as industry public chain, industry alliance chain, decentralized application and developer community.

Zorro can be likened to a mutual trust business collaboration engine, which promotes a credible and safe business environment for all participants in the ecology. In such a business environment, the collaboration friction between all business entities will be greatly reduced, thus making all business collaboration more efficient and reliable.

2. Zorro ecological promotion

The market has already proved that it is impossible to realize the large-scale commercial landing of blockchain by simply playing the financial attribute of blockchain and encouraging the early participants. Zorro has done a lot of practical and theoretical research in the fields of finance, e-commerce, marketing, games, AI, IoT, etc. It is committed to providing the underlying technology infrastructure, providing the ecological participants with the traditional information technology connectivity, the large-scale business application implementation path, and building a new financial infrastructure.



2.1 Zorro decentralizes financial services

DeFi, decentralized finance, is one of the best scenarios for blockchain technology. The core principle of DeFi is to provide a new, permitless financial services ecosystem, without any centralised authority, that anyone in the world can use. In this ecosystem, users are the custodians of their assets, with complete control and ownership over their assets, and they have free access to all the decentralized markets on the market. DeFi's most important vision is to equalise all assets, to create a more open financial system by trading across borders in the global market. On the one hand, the development of Defi business will overturn the existing organizational structure and business model of the financial industry, and realize the "de-banking integration and self-integration"; On the other hand, it will improve the liquidity of mainstream digital currency and expand the value recognition, so that it will eventually become a stable "currency" and construct a new commercial and financial system. This provides the real pratt & financial feasibility, let every man, every enterprise credit into wealth Banktheunbanked, Servetheunderserved.

Currently, DeFi is still in its early days, but its development space is unimaginable. To be successful with DeFi changing the future requires not only the development of a rich and valuable application product, but also the large-scale use of hundreds of millions of users and the absolute security of almost "zero errors". Zorro, as the future global trusted settlement layer, is to provide the world with a set of low-cost and efficient payment and settlement system, to meet the requirements of efficient payment and transaction, and to ensure the absolute security of the entire distributed book, to build the distributed financial infrastructure.

Decentralized financial products are often popular demand, such as decentralized insurance, decentralized lending and so on. Zorro USES a layered, multilevel architecture to support unlimited scaling of performance, storage, and applications. All industries can develop DeFi application based on Zorro to meet market demand on their own business basis, and realize efficient lending, transaction and payment for a large number of users.

1. Flexible combination of protocols

The key innovation of DeFi is the modularization of the basic elements of finance and the commercialization of trust through this modularization. Zorro itself will develop a series of underlying agreements, such as wallets, payments, identity and asset issuance, and introduce an increasing number of open financial agreements. The application layer can come from the protocol layer needed by the combination and realize the application landing according to the gene of its own team and the discovery of market opportunities. For example, a decentralized exchange can be implemented by a combination of wallet agreements, loan agreements, custody agreements, and exchange agreements.

2, safe and reliable

DeFi business involves the transaction and storage of a large number of digital assets, and its security issues are particularly important. Zorro USES a hierarchical consensus stack to secure protocols, contracts, data, networks, and more.

3. Good user experience

DeFi is essentially an application that helps users solve problems and create value and needs to ensure a good user experience. Zorro has dynamic and scalable computing and storage capacity, TPS can be easily extended to 10W, short validation time, and effectively solve network congestion problems; Zorro USES an ultra-low fee model that does not shift the burden of accessing network resources onto users. And Zorro USES a variety of ways to store data, in the face of mass data can be quickly read and processed.

Kevin kelly says that finance should evolve into a way of life, and that only by integrating it into every aspect of people's lives can it be truly transformed. In the future, more and more commodities will be created through blockchain open cooperative organizations in human commercial activities, including more and more digital products such as culture, entertainment, games, etc., and the financing needs generated in the process of commodity creation will be solved through the financial services on the chain, and finally through the "currency" of blockchain to pay. It would be a disruptive change in human business and financial systems. Zorro offers this possibility with decentralised finance, which aims not at decentralisation itself but at greater openness and equity. The development of DeFi will positively promote the ecological development of Zorro:

4. Attract lots of developers

The variety of DeFi application scenarios and the expectation of high future growth will attract a large number of developers and projectors to develop based on the frameworks and modules provided by Zorro.

5. Attract a large number of users

DeFi has no barriers to entry, no fear of privacy being vetted and exploited, and the advantage of all data being open and transparent allows users to participate more widely in the way wealth is distributed and grown in the new era. The continuous expansion of user scale is encouraging the development of more meaningful and valuable applications.

6. Effective energizing

DeFi is the blood of the trusted world digital economy, which can promote the prosperity and development of DAPP and application chain developed based on Zorro. In Zorro ecology, various applications are interconnected and integrated, so that capital flow, information flow, trust flow and logistics flow on and off the chain can be integrated, and accelerate the wonderful blooming of the distributed business world.

2.2 Zorro decentralized user system

The trusted collaboration network based on Zorro, the real ID system of Zorro and the trusted settlement system of Zorro are bound to cause a new marketing revolution.

Current commercial subject Value growth of the main driving factor is transformed into the Value of their own user growth, and technology makes the user can be provided by Zorro Value stored in the distributed network, finally also can complete integration, provides a feasible Customer Value Management model, we defined it as a CVM (Customer Value Management).

The CVM can also be understood as a new user loyalty revolution that capitalizes all of the user's behavior and can aggregate and permanently store the user's value. We will provide each user with a private value memory (excluding assets, but also some core private data).

Under the new marketing system, the traditional pull and hold models have changed dramatically:

1. From the original commercial subject's active penetration and encouragement and passive acceptance by users, it is gradually transformed into the value growth driven by users themselves. Users will join the value network (also defined as community) more autonomously because their personalized value is recognized.

2. Retention: from the maintenance and encouragement of more unilateral subjects of the original commercial subjects, it is gradually transformed into the continuous interaction between users and commercial subjects to form a common value community, and users become more loyal because of the value precipitation.

With the growth of the common value of users and business entities, the value transmission between their value networks is promoted, and this interaction is to establish a business environment of mutual trust at the bottom, so that the most basic marketing activities, such as traffic exchange, advertising, become no longer worry about traffic trap, settlement risk.

Future products and services will continue to upgrade, but marketing will always be an inevitable problem for business activities. The trust marketing network based on

Zorro technology will greatly reduce marketing costs and cover a wider range more efficiently.

2.3 Zorro distributed e-commerce

Distributed e-commerce refers to the construction of a credible equal supply and demand network based on Zorro block chain technology. In this network of mutual trust, the behaviors of each participant are capitalized according to the agreed standards, and they can independently cooperate and exchange value according to the agreed rules.

With the rise of social e-commerce and the in-depth exploration of private domain traffic in recent years, it seems that there is no structural innovation in the e-commerce market. In fact, from the macro perspective of both supply and demand:

1. Supply side: industry network coordination has not yet been formed, and there is great potential to improve efficiency through integration.

2. Demand side: consumer demand changes from the public to the individual, and personalized consumption gives birth to the flexible supply chain.

Based on the pain points at both ends of supply and demand, Zorro's core goals for distributed e-commerce are as follows:

1. A collaborative supply network is formed through the integration of the supply side through the block chain technology: in the aspects of idea, production, processing, pricing, sales (pre-sale, formal sales), each participant conducts independent cooperation and decides the final revenue according to the value of contribution.

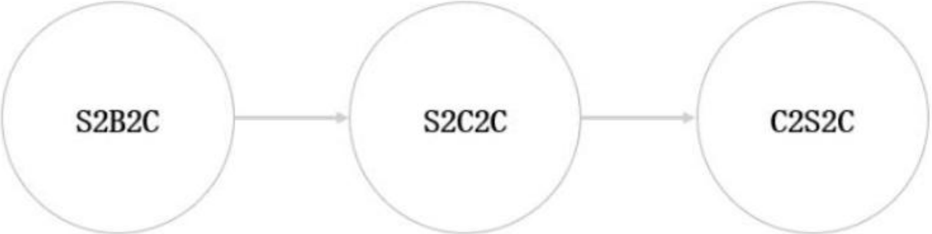
2. Based on the consensus standard, users' behaviors are capitalized and stored on the block chain to form a new value network. The continuation of value can protect users' personality and stimulate their personality.

3. Because of the common value body, the user (demand side) is further bound to the supply side, so the smart contract can guarantee the benefit distribution among different participants.

In such new trust distributed eb point road, participate in the characters of the collaboration of friction greatly decreases, and thus greatly improve efficiency and reduce the cost of trust at the same time, the new marketing revolution of Zorro gives the entire new business potential energy eb point road, makes the value of each role has been more reasonable allocation and be stored and the independent ability to realize their upgrade, role conversion.

1. Users: from a simple consumer to a value investor, consumption is investment, which can be direct money, can be social relationship assets, can be behavioral assets and so on.
2. 2, server: (sales, customer service, more professional division of cutting on content producers), engaged in more in line with their respective personality product service work, the provider of service experience, creating content and operation data such as capitalization, and stored in a wider range of values within the network, server service boundary has been broken.
3. 3. Brand owner: brand is a consensus asset with economic value. In the new business environment of mutual trust, the brand owners and users jointly create and maintain the brand and share the brand benefits, which makes the growth path of the brand shorter and more stable.
4. 4. Producers: they can more truly and comprehensively grasp the data in the whole supply and demand network, and then achieve on-demand production and customization, so as to make it closer to the personalized consumers while ensuring sufficient production efficiency and extremely low waste.
5. 5. Developers: the data is separated from the program, the data ownership is returned to the users themselves, and the developers' profit model of collecting user data is changed to a new model of co-creating value with users.
6. As the dominant position of user value is gradually enhanced, the evolution of

distributed e-commerce mode is promoted synchronously:



7.

8.

9. In zorro-based distributed e-commerce network based on mutual trust, S refers to the super supply chain platform integrated by block chain technology. Under this integration, S2B2C is no longer a simple variation of B2B2C, but a collaborative network ecosystem based on technology chain and data-driven. The traditional supply chain is all linear thinking, such a supply chain can not cope with the three completely conflicting core indexes of low cost, fast response and high customization at the same time, only the structure of trusted network has enough flexibility to realize the dynamic optimization of these three indexes. The industrial value collaborative network built by blockchain is beyond the reach of any single industry. The value of the platform is the formation of the network and the underlying architecture. From the perspective of empowerment, it breaks through the "transaction" thinking of the traditional alliance system and realizes the symbiosis and win-win of S and all kinds of small B in the industrial chain. As the value of the user grows, the role of the user becomes more and more important.

This evolutionary pattern does not mean to directly overthrow all resource-dominated formats, but is a form of fusion pattern for a long time. However, in the distributed e-commerce network built by Zorro, each role can carry out mutual trust and cooperation on a larger scale, and jointly create a greater commercial value community.

6 TOKEN ALLOCATION

TRUE FREEDOM IS THE FREEDOM TO DO WHAT YOU SHOULD DO WITHOUT GAINING WHAT YOU WANT.

-MONTGOMERY

ZORRO BLOCKCHAIN

TOKEN ALLOCATION

Circulation: 330 million

Distribution ratio:

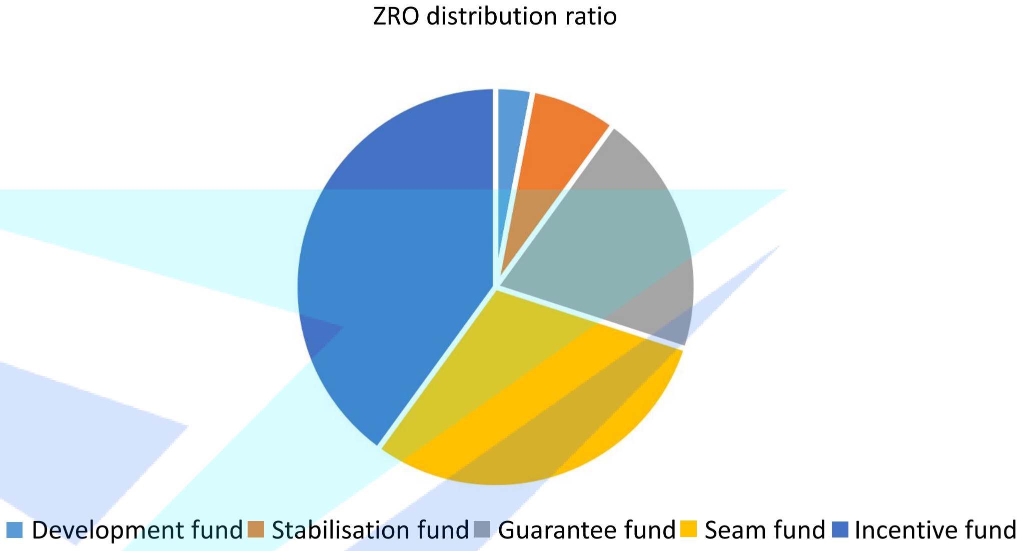
3%, development fund;

7%, stabilization fund;

20%, security fund;

30%, ore bed fund;

40%, incentive fund;



The 20% security fund has 66 million certificates, and 6,600 are released every day. All the ETH purchased in this part flows into the verification pool to provide security for investors. After the collision of development funds, the security fund is released. The development fund is used for the currency of the whitelist exchange, media publicity and distribution, multi-ecological construction, etc. The incentive fund is opened, the consensus foundation is formed,The autonomous league club will gradually buy back the initial release of the money (9.9 million pieces) and put it into a black hole for permanent destruction. The stabilization fund is used for the common value and ecological maintenance, and the incentive fund is used for the incentive of the monetary calculation and the promotion of calculation. The ore layer fund is frozen in the early stage, upgraded in the late stage and used for mining after mapping.

7

TEAM

AS LONG AS YOU ATTACK WITH THE SWORD OF JUSTICE, EVEN THE WEAKEST ARM WILL BE INFINITELY POWERFUL.

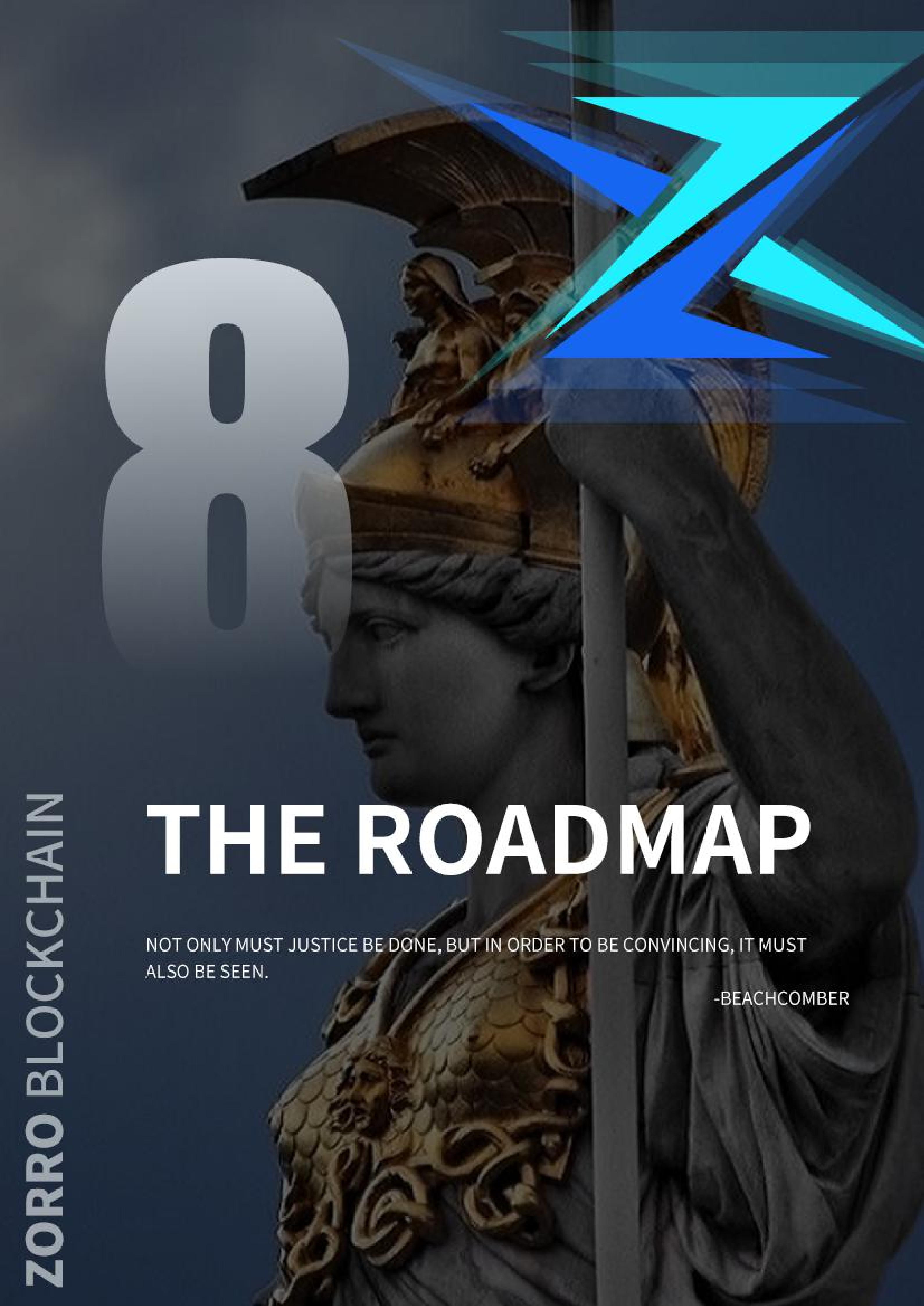
——WEBSTER

ZORRO BLOCKCHAIN

TEAM

Zorro originated from the reflection on the pain points of the global digital economy and real economy. Zorro's main operating ideas are deeply inspired by the operation mode of dark network. The dark web (invisible web, hidden web) is a collection of resources stored in an online database that cannot be accessed via hyperlinks but needs to be accessed via dynamic web technologies. It is not a surface network that can be indexed by standard search engines. Michael bergman likens search services on the Internet today to pulling up a large web on the surface of the earth's oceans. Much of the surface information can be found this way, but much more is lost by search engines because it is hidden in the depths. The vast majority of this hidden information is web information that must be generated by dynamic requests and cannot be found by standard search engines. Traditional search engines cannot "see" or capture the content that exists on the dark web, except through a specific search of the pages. By contrast, the dark web is hidden -- and Zorro's team is a group of talented hackers from the top of the dark web ecosystem!

Zorro, why is this project called zorro? Because the current environment is affected by the epidemic, virus, political environment and so on, resulting in the people's livelihood, people's depression, pain, despair, so a group of technical geeks as the messenger of justice, like zorro light the sword of justice, justice, freedom, equality, so the team is called zorro.



8

THE ROADMAP

NOT ONLY MUST JUSTICE BE DONE, BUT IN ORDER TO BE CONVINCING, IT MUST ALSO BE SEEN.

-BEACHCOMBER

THE ROADMAP

2017.06	Zorro creation team was established
2018.01	Zorro's underlying core module has been developed
2019.03	Zorro application layer module is perfect
2019.06	Smart contract deployment on the Zorro chain
2019.08	Zorro global primary node deployment
2020.01	Zorro test online line, global dark net internal test
2020.02	Zorro white paper released
2020.03	Zorro global consensus program launched
2020.04	Zorro sword program
2020.06	Zorro wealth freedom program
2020.08	Zorro just war plan
2020.12	Zorro peace tour program
2021	Zorro stars flourish

9 DISCLAIMER

ALL KNOWLEDGE THAT DEVIATES FROM FAIRNESS SHOULD BE CALLED CUNNING, NOT WISDOM.

-PLATO

DISCLAIMER

The documents are for information purposes only and are for reference only and do not constitute any recommendation, solicitation or solicitation for the sale of shares or securities by Zorro or its related companies. This document does not constitute nor is it understood to provide for any sale or purchase, nor is it a contract or commitment of any kind.

Given the unpredictable circumstances, the objectives set out in this white paper may change. While the team will strive to achieve all the objectives of this white paper, all individuals and groups that purchase Zorro will do so at their own risk. The document content may be adjusted in the new whitepaper as the project progresses, and the team will make the updates public through announcements on the web site or the new whitepaper.

This document is intended to be used only to communicate information to specific audiences who request information about the project and does not constitute any future investment guidance or any form of contract or commitment.

Zorro expressly disclaims any direct or indirect losses caused by the participants, including: once the participants participate in the Zorro distribution plan, they express their understanding and acceptance of the risks of the project and their willingness to personally bear all the corresponding consequences. The project team makes it clear that it does not promise anything in return, nor is it liable for any direct or indirect losses caused by the project. The Zorro involved in this project is a virtual digital code used in the transaction process and does not represent the equity, revenue or control of the project. Due to many uncertainties in digital assets (including but not limited to: the general environment in which countries regulate digital assets, the industry encourages competition, and the technical loopholes in digital assets), we cannot guarantee the success of the project. There is a certain risk of failure for the project, and Zorro has the risk of zero.

Although the team will make efforts to solve the problems that may be encountered in the process of project promotion, there is still policy uncertainty in the future. It is important for everyone to understand all aspects of blockchain before support, and participate rationally on the premise of fully understanding the risks.The team will strive to achieve the goals mentioned in the document, but the team cannot make a full commitment due to the presence of force majeure. To the maximum extent permitted by applicable law, the team shall not be liable for damages and risks arising from its participation, including but not limited to direct or indirect personal injury, loss of business profit, loss of business information or any other financial loss.