Zoro

In People We Trust
Intro

Moving towards a fully digital human society

Since the rise of the Internet in late 1990s, human society has experienced the Internet 1.0, 2.0, and mobile Internet era. The Internet has moved from elite to ordinary people. The number of data on the whole network has increased from GB to TB, PB to EB. With the advent of 5G and IOT, Internet will expand from people to things, regardless of the number of connected devices or the amount of data, will further explosive growth. In future human society, from personal life, production management to national governance, all aspects will rely more and more on digitization. These nodes and data need a safe and reliable underlying guarantee, based on asymmetric encryption, and Blockchain technology is the best solution for this guarantee. In the era of intelligent economy, blockchain technology is also necessary.

Future computing

With the continuous growth of Internet infrastructure and the arrival big data era, more and more computing will occur in cloud servers in the future. Cloud computing is the trend of future, but the centralized cloud is built by hardware and operating systems that are constantly patched by PC era. There are many problems, C/S structure in PC era is a client-server architecture developed from personal desktop computers, it does not consider a large number of computing nodes and data work together today. When 5G era arrives, everything will be rewritten, and we need a new system that is really focused on the era of Internet of Everything to support future computing.

At present, centralized cloud is established by each company. It is a fragmented, untrusted cloud computing. Cloud computing in future should be composed of various public clouds, private clouds, and various computing devices. Computing resources are readily available. And a set of open and secure trusted computing networks that
works everywhere, just as the Bitcoin network operates every day, it extends to all computing, not just ledgers. All of these will be a new computing system that blockchain technology can bring.

**Blockchain in future**

In recent years, rapid development of blockchains has emerged a large number of public networks with different technical ideas and perspectives. However, compared with other mature fields, blockchains are still in the early stage, and their technologies and applications are far from mature. We are optimistic that more and more talents joined the industry. For the foreseeable future, major companies, industries and even some sovereign countries will formulate their own blockchain standards and plans. It is not to worry that a certain numbers of public chains will disappear, stronger and better public chains will born. With in-depth application of blockchain in various fields, The prototype of new computing system will gradually emerge as what we are expected.

One problem is that if each public chain is politically independent and its barriers are not broken, then each public chain will become an isolated information island, and the future computing network what we are expecting will never exist. Therefore, the cross-chain will be a major theme of future blockchain, how to exchange data between different public chains and applications requires a set of recognized solutions, which can be called a public chain bridge, or a "public chain" of the public chain.

Another problem that lies in front of us is that the exploration of industry applications is still urgently needed. There are already many good analysis and assumptions about the future role and positioning of the blockchain, but compared to the thousands public chains we already have. For public chain projects, there are few real blockchain applications that can be used and have practical application scenarios. As a prospect for blockchain technology in the near future, we believe that blockchain technology for some vertical applications will be more valuable. It can be used as an entry point for the practical application of blockchain, gradually exerting its technical
value and conversely promoting its technological development, thus making blockchain technology a big step forward.

Game-A fully digital world

Regarding the vertical field, game industry is what we want to focus on is also the focus of Zoro. The development of video games has become a global industry with an annual output value of 100 billion US dollars only takes several decades, the number will be further magnified. If calculated the value of tokens in the beginning of 2019, it is equivalent to re-creating a bitcoin network every year.

In mobile Internet era, a large part of game's annual output value flows to the virtual assets in the game, and the current game industry operation mode (project, R&D, publishing and distribution mode) is not in an efficient and ideal state. Blockchain technology can revolutionize the entire industry (see BlatCat case section for details).

For blockchain field, the game world is a fully digital world. Game assets and attributes naturally match the characteristics of blockchain. After finding the entry point of both blockchain and game, the industry will usher in the explosive growth.

Zoro

Cross-chain application solution focused on digital (game) world

Zoro includes ZoroChain and ApplicationEngine. ZoroChain is a cross-chain solution consisting of RootChain, MappingChain and ApplicationChain. ApplicationEngine is a set of .NetCore-based application runtime environment built on ZoroChain. ZoroChain's computing resource node, Application Engine provides a set of distributed computing runtime environment for applications, applications can easily access the blockchain network and call various computing resources in the network.
The goal of Zoro is to build a cross-chain distributed computing network environment based on blockchain technology for the vertical field of game industry. Blockchain technology can meet the development needs of game industry in terms of operational efficiency and functional modules. Developers can easily and efficiently develop and release blockchain games, providing a one-stop cross-chain solution.

**ZoroChain**

**ZoroCore**

ZoroCore is the core of ZoroChain, and the core basic module for providing blockchain computing services such as consensus, verification, and block persistence for all other modules in Zoro.

**SpringThunder Consensus:** ZoroCore provides a set of Spring Thunder Consensus (ST Consensus) algorithm based on node reliability weighted VRF-BFT. The main idea is to evaluate the node reliability by algorithm, and replace the common node election work with other public chains by reliability order, or it can be said that the machine algorithm replaces the work of manually electing nodes. We believe that the machine will be more reliable than humans when the right algorithm is selected.
In STC algorithm, the reliability of the node will be affected by two important parameters, one is the node mortgage, and the other is the work integral proof. The two determine the reliability order of the nodes. STC will use VRF-BFT algorithm to select node by the weight of the nodes according to nodes reliability, while providing a monitoring mechanism to penalize cheating to further improve security.

**Node Mortgage:** If you need to participate in the consensus, you must first become a node, and the node needs to mortgage a certain amount of tokens. One node can have multiple token holders to participate in the mortgage. The token holders who do not want to be a node, they can mortgage their tokens to other nodes, and share the proceeds. If the node makes a mistake, users may suffer the risk of losing token. Please see chapter ZID for more details.

**Proof-of-workload:** The historical participated transaction confirmation and consensus block will be converted into points and accumulated to the node. The proof-of-workload is the record to prove the node's stable participation in the network contribution, and is an important parameter for block competition of the node. Work score is adjusted once every 604,800 blocks (about a week). The adjustment algorithm is: NewWorkload = 0.9*OldWorkload. By adjusting the algorithm, nearest integral weight can be kept higher than historical one.

![Graph](image)

Each period integral decreases with time.
**VRF-BFT:** The full name of VRF-BFT is Verifiable Random Function – Byzantine Fault Tolerance, which can verify the stochastic function Byzantine fault-tolerant algorithm, which is used as the consensus algorithm in STC. The list of all nodes in the network will be sorted by $F_x$ (mortgage, proof of worklod). Each time competing for account right, the first 100 nodes in the list (at least not less than 4, otherwise the consensus fails) will be taken as the candidate node for VRF-BFT consensus.

The consensus process is outlined below:

1. When block is generating in each round, all nodes will update the node list by $F_x$ (mortgage, proof of work points);
2. According to VRF algorithm, select one proposal node from the top 100 nodes in the list to make a proposal;
3. According to VRF algorithm, multiple verification nodes are selected from top 100 nodes in the list to verify the proposal;
4. Including the proposal node, If more than 2/3 of the nodes pass the verification, the proposal node will broadcast that the block is generated. Otherwise, repeat step 2 and re-select the proposal node.
Punishment mechanism

For confirmed transaction, if there is any objection, monitoring node may initiate verification. The verification transaction shall submit the deposit, and the candidate node of the whole network shall vote for 2/3 or more. If the verification fails, the monitoring node's deposit will be deducted. For different degrees of error, a certain percentage of mortgage tokens will be deducted to the monitoring node and a certain percentage of work points will be cleared.

1. The verification transaction will be verified in the transaction pool, voted and recorded in the current block by the proposal node and the verification node in each round of consensus;

2. When a verification transaction has more than 67 candidate nodes voting true or false, verification penalty is executed after voting.

3. When a node has an authentication request for an incomplete tag, its mortgage token cannot be released.

4. If the node is judged to be cheating, it is necessary to deduct the node mortgage token of max (the transaction value token, 1% of mortgage token), and deduct the corresponding workload calculated by the token. Deducted token will reward to the monitoring node account.

5. When the verification transaction is initiated, the monitoring node shall submit max (100, the same deposit of the transaction value token). If the node is judged to be not cheat, the deposit will be forfeited and fed back to the verifying nodes.

ZoroChain Chans

ZeroChain consists of three separate parts, each of which is one or more independent ZoroCore-based chains, and they are: RootChain, MappingChain, and ApplicationChain.
RootChain

RootChain is the root chain of ZoroChain. There is only one in the whole network. MappingChain and ApplicationChain are managed by RootChain. The internal cross-chain transactions of ZoroChain need to be completed through RootChain. For details, see chapter “Application Chain Cross-Chain” in ApplicationChain.

The rootChain node is called "core node", which constitutes the core network of ZoroChain. The permission and security level of RootChain is the highest in ZoroChain.

MappingChain

MappingChain is the mapping chain of ZoroChain. The data of other public chains will be merged into ZoroChain through the mapping chain. Each public chain corresponds to one mapping chain. The mapping chain consists of two types of nodes. The verification node and the observation node, verification node must be run simultaneously ZoroChain and the public chain program (such as mapping ethereum, you need to run the geth software), verify that after receiving the new block data from the public chain, the node will convert the other public block data into the MappingChain data according to the format set by ZoroChain. The MappingChain performs the second STC consensus. After consensus is confirmed, it will broadcast to other nodes. The observing node does not need to run the public chain program, and it only receives the consensus data of the synchronization view verification point. A node can be both an observing node and a verifying node.
**Data Mapping**: Similar to the side chain, MappingChain creates a parallel side chain with the main chain. The difference is that MappingChain will "translate" the public chain transaction data into the ZoroChain space, and the transaction data format will be converted into Zoro. The format (usually the transaction result set, temporarily unable to synchronize non-standard transactions or non-standard smart contract operations), after the mapping is completed, in addition to the data of the cross-chain trading part, all transaction data in the public chain can be passed inside the ZoroChain space through MappingChain and get a quick verification.

**Second Consensus**: The verification node of MappingChain will obtain the public chain transaction data and block data through other public chain interfaces. The acquired data will be converted into ZoroChain format and broadcast in the MappingChain network. Based on ZoroCore's STC algorithm, the second consensus
will be made and the block will be generated. The transaction of the public chain will
not be executed again on the MappingChain, but will be translated into a result, and
then agreed, recorded on the MappingChain.

For example, if there is a transaction in which 20 ERC20 tokens named XCoin
are transferred from account A to account B on Ethereum, the transaction process on
Ethereum is executing the token smart contract through EVM, and it will be
completed by put process to change the storage area; then the transaction in the
second consensus of MappingChain process will not execute EVM smart contract, but
simply convert to the value of account A under the XCoin address minus 20, the value
of Account B under the XCoin address plus 20.

The MappingChain startup phase only supports standard transfer transaction
mapping for public chains, including standard token contract transaction mapping for
each public chain, and will be extended to NFT and other widely adopted
standardized contracts in the future.

**Security Issue:** The security of MappingChain depends on the number of
verification nodes. The larger number, the higher the security. At the same time, it
depends on the number of mortgage tokens. Generally, the MappingChain's
verification node cannot verify transactions that exceed its mortgage token amount to
easure cross-chain transaction funds security.

**Cross Chain with Pub Chains:** When users need to map their assets to
ZoroChain, their assets can be transferred to the mapping contract or account on
public chain. When the MappingChain detects the transaction, the token on the
Zorochain will be issued to users accounts through the verification node consensus.
Conversely, when users need to transfer the mapped asset back to the public chain, the
mapping token transaction is sent to the MappingChain. After the node is verified, the
mapping contract or account token on the public chain is transferred back to the
public chain user account. If the monitoring node finds that the verification node is
cheating, it can initiate re-authentication. If more than 2/3 nodes pass, the equal
amount of deposits of all the cheating verification nodes will be deducted and rewarded to the monitoring node. If the verification fails, the monitoring node deposit will be forfeited.

The public chain assets will be decentralized through the super-verification node. Zoro will deploy mapping contracts on each public chain. The contract will be used to manage the assets transferred to MappingChain. The contract will be managed by using a multi-verification node multi-signature mode (see "ZID and Nodes" section for more details), which will maximize the security of ZoroChain mapped assets in a decentralized manner.

How to transfer assets from public chain to Mapping Chain?

1. Account A (public chain address) initiates transfer of TxP1 in public chain and transfers 10 NEOs to the mapping contract;

2. Account Az (ZoroChain address) initiates a token mapping transaction TxMap in MappingChain, including TxP1 transaction information and NEO public chain signature of account A;

3. The verification node verifies the TxMap, and verifies the TxP1 transaction information and the signature of account A by mapping the data of public chain, and then distributes 10 mapping NEO tokens to account Az to complete the mapping.
How to transfer assets from MappingChain to public chain?

1. Account Az (ZoroChain address) initiates mapping token destruction transaction TxRed in MappingChain, destroying 10 mapping NEOs, including public chain account information of account A;

2. The verification node verifies TxRed and freezes 10 mapping NEOs in account Az;

3. After freezing 10 mapping NEOs in Az, super-verification node will construct a public-chain transfer transaction TxP2 and broadcast a multi-sign request;

4. After multi-sign process is completed, TxP2 information will be updated to TxRed. 10 freeze mapping NEOs in Az will be destroyed. At the same time, TxP2 will be submitted to the public chain, and 10 NEOs will be transferred from the public-chain mapping contract to account A to complete the extraction.

ApplicationChain

ApplicationChain is the application chain of ZoroChain. It mainly serves the application, and the application chain is composed of multiple parallel chains. It can be created and queried through the root chain, it has a high speed (milliseconds). If there is no request for a period of time, block will not be generated. Application chain transaction requests do not need to wait for each other and can be concurrent. When
an application chain fails or under attack, it will not affect other application chain operations.

The cross-chain of application chain: Similar to the cross-chain of public-chain assets, it needs to be completed by the verification node, the monitoring node is responsible for post-supervision and punishment, and the application chain asset transfer needs to be completed through the root chain. The application chain cross-chain verification node needs to acquire the block data of both application and root chains at the same time, and the application chain verification node manages the asset mapping contract on the root chain in a multi-signature manner.

The application chain, the root chain, and the mapping chain all use the same address encryption algorithm, so they can mutually verify transaction information.

How to transfer assets from the root chain to the application chain?

1. Account A initiates transfer of TxP1 in the root chain and transfers 10 ZOROs to the AC1 mapping contract;

2. The application chain AC1 verifies that after the root chain checks to TxP1, AC1 on application chain initiates a ZORO issuance transaction TxSend1, which contains TxP1 information;

3. Consensus node of AC1 on application chain verifies TxP1 and TxSend1 respectively, and after passing, 10 ZOROs are issued to account A from AC1 on application chain.
How to transfer assets from the application chain to the root chain?

1. Account A initiates 10 ZORO transfers from the application chain AC1 to the root chain transaction TxTrans1;

2. The application chain AC1 consensus node freezes 10 ZOROs of account A according to the TxTrans1 transaction;

3. After the freeze process is completed, the verification node will construct a root chain multi-sign transfer request TxP2 and broadcast it;

4. After multi-sign process is completed, the verification node updates TxP2 information to TxTrans1, and destroys 10 ZOROs in account A on the frozen application chain AC1, and submits TxP2 to the root chain, then 10 ZOROs map the contract account from the root chain AC1 Transfer to account A.

The virtual machine of application chain: The smart contract virtual machine of application chain can support OnChain and OffChain computings. As the name implies, OnChain computing is consistent with other smart chain virtual machines of other public chains. The contract call transaction needs to be executed by all nodes and change the chain according to the smart contract execution result state, and the difference between the OffChain computings is that the transaction body contains the execution result of this call in addition to the calling contract, method, and
parameters. After the other nodes receive the OffChain computing, smart contract call will be executed asynchronously, simply synchronize the execution results.

The security of Offchain computing: Since the OffChain computing does not verify the computing process between nodes, the side effects caused by greatly improving the synchronization efficiency are obvious, and the security will be greatly reduced. Only the monitoring node can perform post-mortem monitoring, so in general, we recommend to place the lower security requirements in the OffChain computing. Although its security is much lower, the relatively centralized service, after all, has an after-the-fact supervision part, and the security is still higher than the centralized service.

**ZID and its nodes**

If you want to join the ZoroChain network, you must apply to become a node. The application is automatically confirmed by the network. The nodes are divided into core nodes, observation nodes, application nodes, monitoring nodes, and verification nodes.

**ZID:** Before becoming a node, you must create a ZID. Users can create a ZID by initiating a ZID creation transaction. The ZID transaction requires a fixed fee of 10 ZOROs.
ZID is the identity of users in ZoroChain network. To participate in the network construction of ZoroChain, such as participating in governance voting, obtaining proxy revenue, becoming a node, etc., ZID is indispensable.

After obtaining the ZID, you can use the collateral token to run various nodes, or mortgage token to other nodes to share the node revenue.

**Core node:** To become a core node, you need to mortgage at least 100,000 ZORO, you can participate in sharing core node mining rewards, the core node can participate in RootChain block producing competition, and obtain core node mining rewards. For details on mining incentives, see “Mining”.

**Observation node:** No need to mortgage if you want to become an observation node.

**Verification node:** Becoming the verification node needs to mortgage at least 100,000 ZORO, it can participate in MappingChain block producing competition, and obtain the verification node mining reward; becoming the super verification node needs to mortgage 1,000,000 ZORO. The only difference between the super verification node and the verification node is that it can participate in the public chain token and multi-sign management. To become a super-verification node, you need to review it and initiate a super-verification node application. The application will be approved by the existing super-verification node.

**Application node:** Becoming an application node, you need to mortgage 10,000ZORO, which can share the operating fee income of the application chain.

**Monitoring node:** Becoming a monitoring node, you need to mortgage 1,000ZORO, you can initiate a transaction verification request, and you can get the deposit bonus deducted by the node.
ApplicationEngine

ApplicationEngine is a .NetCore-based application virtual machine. It works on the ApplicationChain in ZoroChain. It interacts with ZoroChain through the application chain. The node running by ApplicationEngine is defined as a computing node. Its functions can be extended through the plug-in system. The main modules include network communication, a general-purpose computing library, a graphics computing library, a database, etc., an application can run on the ApplicationEngine, and its computing nodes can set up or lease other nodes set up by other users.

Computing node

Computing node is the node running by ApplicationEngine, which provides the environment required for the ApplicationEngine to run. Computing node network consists of compute nodes that provide different functions, such as general-purpose computing, graphical computing, AI computing, storage and etc. Connected through application chain nodes into ZoroChain, is the leaf node of the application chain.

ApplicationEngine can record key computing steps to ApplicationChain through OffChain computing, and can also perform various chain operations and smart contract calls of ApplicationChain through OnChain computing.

The running cost of computing node can be settled through the application chain, and the fee settlement is specifically referred to the “node incentive-system fee” section.

Render Node - Render Stream Video Stream Cloud Computing

As we mentioned earlier, future computing will happen in the cloud. In gaming field, Sony, Micro Soft, and Google have all proposed their own cloud gaming solutions. Of course, they are all centralized clouds, and all of them are using video stream for graphics transmission. Due to the current network environment, user
experience is not good. 5G era is coming, low latency and high bandwidth will make the video streaming cloud game experience better like playing the console game.

Zoro will provide rendering nodes, and the rendering node can choose two kinds of remote graphics data transmission schemes: rendering stream and video stream.

Rendering stream scheme means that after the CPU completes the computing, the GPU performs partial computing, and generates the rendering instruction stream and send it to remote client, and the client local GPU continues to perform rendering according to the rendering instruction and further rasterizes the display, and the GPU needs the rendering material is pre-stored by the local client and loaded to the GPU.

Video stream solution means that after the CPU completes the computing, the GPU performs rendering and outputs the rasterized graphics data, and submits it to the video compression module, then outputs the real-time video stream to the remote client, and the remote client performs video decompression display.
Rendering stream requires less cloud computing, lower bandwidth, higher performance requirements for local terminals, and requires GPU; Video stream requires more cloud computing, higher bandwidth requirements, lower performance requirements for local terminals, and no need to use GPU.

The applications of ApplicationEngine can send graphical data through rendering nodes, and both stand-alone and multiplayer games are executed and rendered on the server. Through the appropriate digital copyright mechanism, stand-alone games can better avoid piracy in the case of cloud games; multiplayer online games can be freed from the system architecture of C/S structure, developing multiplayer games as easy as stand-alone games, and work remotely. Decentralized to the graphics transfer and input command transfer level, greatly simplifying the development work.

**Open-source game framework**

Based on Application Engine, Zoro will build a series of open source game frameworks that will cover various types of games (such as FPS, RPG, RTS, SLG, MOBA, etc.) for various terminals. Open-source game framework will be freely available to the community, greatly reducing the development costs of game developers, while greatly enriching the application contents of Zoro community.

**Node incentive**

**Mining**

ZoroChain will provide token incentives for the participating nodes, ie mining, MappingChain and RootChain in ZoroChain will have mining output, as follows:

**MappingChain mining**: The MappingChain node yields 50% of the output to the proposal node (ie, block producing node), 40% to the participating consensus nodes, and 10% to the mining pool of MappingChain.
**RootChain mining**: The RootChain node outputs 50% of total blocks to the proposed nodes (ie, block producing node), 40% to the participating consensus nodes, and 10% to the mining pool of RootChain.

**Mining pool**: Each cycle of MappingChain and RootChain's mining pools (604,800 blocks, about 1 week) will select the top 10 rewards in the node workload list, and they will get 30% of total tokens in mining pool, and then randomly select 10 nodes in the list to reward 10% of total tokens in mining pool.

The mining of ZoroChain will be launched in Zoro Ver 2.0.

**System fees**

1. Charge for creating ZID: 35% of the total ZID creating charge will reward the proposal node (ie, block producing node), 35% of the total ZID creating charge will reward the participating consensus node, and 30% of the total ZID creating charge enters the mining pool of RootChain.

2. Gas fee: Gas fee of Root chain and mapping chain will be calculated by Gas Price*Gas, 35% of the total Gas fee will reward the proposal node (ie, block producing node), 35% of the total Gas fee will reward the participating consensus node, 30% of the total Gas fee will enter the mining pool of RootChain; the charge of application chain will also be calculated according to Gas Price*Gas, the paying account can be specified by multi-sign method, 50% of the application chain charge will reward the proposal nodes (ie, the block producing node), and 50% of the rest will reward the participating consensus node.

3. Monitoring node verifies the transaction deposit: if the deposit is deducted, it will enter the mining pool that the verification node belongs.
4. Voting proposal deposit: A certain amount of deposit is required to initiate a proposal. If the proposal is voted as invalid, the deposit will enter the mining pool of RootChain.

5. The usage fee of ApplicationEngine (computing node): ApplicationEngine usage fee can be specified by the node builder, two ways can be used: pay according to the computing amount, pay by time (monthly), and the fee is paid to the computing node account. Computing node can also set up a free application Hash, and formulating application can be used without paying for the node. This method can be used when the users build the computing node by himself.

**Token issue**

**Token**
Name: ZORO
Total Amount: 20 billion
Token Distribution: 18 billion of tokens will be mining, 2 billion of tokens will be pre-mining.
Mining output

For total mining output, 50% is allocated to RootChain, 50% is assigned to MappingChain, and the MappingChain is distributed proportionally by MappingChain in current ZoroChain network.

The mining output of ZoroChain will be adjusted according to the number of core nodes. More core nodes, higher reward for the block node. In this way, the supply and consumption can be dynamically adjusted according to the market demand. The demand will increase the production to a certain extent, and vice versa, to keep the balance of both demand and supply.

RootChain and MappingChain have the same blocking mechanism as follows:

- Block generating interval: 1 Sec.
- Decrement interval 12,700,800 (About 147 Days)
- Decrement ratio: 5%
- Initial mining reward: see below

<table>
<thead>
<tr>
<th>Node(s)</th>
<th>Init Prouce(per block)</th>
<th>Init annual output(E)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4</td>
<td>140,160,000</td>
</tr>
<tr>
<td>100</td>
<td>9</td>
<td>280,320,000</td>
</tr>
<tr>
<td>1000</td>
<td>18</td>
<td>560,640,000</td>
</tr>
<tr>
<td>10000</td>
<td>27</td>
<td>840,960,000</td>
</tr>
<tr>
<td>30000</td>
<td>40</td>
<td>1,261,440,000</td>
</tr>
</tbody>
</table>

Management

Governance mechanism

The governance mechanism of Zoro will adopt the governance method of distributed organization of open source community. The core of this mechanism will rely on ZID-based on-chain voting mechanism to implement chain management, and then coordinate various adjustments of Zoro, such as system parameter adjustment.
and rule adjustment. Software node updates and everything related to Zoro's operation can be voted by initiating a proposal.

Voting mechanism is divided into three layers. They are core nodes vote, the verification nodes vote, and the all member vote. Users must provide a deposit for submitting the voting. The voting has four options: consent, disagree, abstention, and invalid. If the voter believes that the proposal is invalid, he can vote for invalid option, if more than half of the votes are invalid, the proposal deposit will enter the mining pool of RootChain pool.

**Stage routemap**

Zoro will have four phases, and they are: closed beta phase, open beta phase (1.0), phase 2.0, and phase 3.0. and:

1. Closed beta phase: This phase focuses on creating ZoroCore and consensus algorithms, optimizing the P2P network structure layer, and improving consensus efficiency. At this stage, test and formal chains will be deployed. Network is not for public join at this stage, and it will be maintained by Zoro team. You can apply for nodes but it is temporarily unable to participate in the consensus, and there is no mining output at this stage. The purpose of deploying a formal network is to continuously test and tune ZoroCore in a complex formal use environment, expose problems, make them more robust and efficient, and the market is the best monitor.

2. Open beta phase (1.0): This phase focuses on creating MappingChain and ApplicationChain to provide mapping chain and application chain services. At this stage, open network nodes will be added in batches. The purpose of batching is to better perform node network. Test, after multiple iterations until the node is completely open to join freely. There is also no mining output at this stage, but work points will be recorded.
3. Phase 2.0: This stage focuses on building ApplicationEngine version 1.0 to realize the basic functions of its computing nodes, such as computing and storage. At this stage, mining output will be initiated.

4. Phase 3.0: This stage focuses on the ApplicationEngine version 2.0, to achieve the computing node expanding functions, and to create the rendering node function.

**Usecase - BlaCat**

**The pain points of game industry**

Centralized traffic and product homogeneity are obvious; the cost of buying online advertisement is high, and it is difficult for small and medium-sized game developers to obtain users; users are very hard to find good channels and get to know their products, small producers and their products are lack of exposure opportunities.

At present, centralized operation mode of game industry has led to the high cost of the circulation link, which has reduced the creative space of developers and eroded the interests of game players; this is an obviously unreasonable distribution mechanism that needs to be considered and changed.

**The pain points of Blockchain industry**

The technical indicators of the blockchain are not mature enough to support complex computing and high-performance applications. Currently, there are no other valuable application scenarios except for token wallet and exchanges.

Even in the two specific application scenarios of token wallet and exchange, users are hard to enjoy the blockchain-technology applications. Responding time on the chain is long, and user experience is bad.
How to change gaming industry by blockchain technology

The combination of blockchain technology and games will not directly make the game more fun, but it will change the game industry and its business model from the following aspects, making the game industry better to "play" and indirectly making the game more fun.

The change of ownership: The most fundamental change bring by blockchain technology to game industry is also one of the natural characteristics of other blockchain applications. It is the change of ownership of the assets. The ownership of game and in game assets are recorded and explained through the chain. The chain does not die, the game and its assets will always exist and be absolutely owned by respective owners;

The change of operation method: Changes in ownership will lead to changes in operating methods. Game development and operation will no longer be provided by centralized vendors, but will be transformed into a core team like volunteers in open source community. Volunteer provides community development and iterative maintenance. The way, and the core team is dynamically variable, as long as the game community continues to be active, community maintain is always active;

The change of profit model: Based on the characteristics of product's community operation, in addition to the first-level digital asset offering, the profit method is more from the circulation of the secondary market and the value-added service, which can focus the teamwork on the users active and asset circulation, rather than trying to increase assets and digging, it will greatly improve the gaming experience;

The change of consumption patterns: Unlike the pure consumption behavior of traditional games, blockchain game behavior will become like investment +
consumption. Based on the changes in asset ownership, operation mode and profit mode introduced above, consumption also means investment for users in a game. More assets they hold, greater influence on the game community. It is a great change to traditional games, the more you invest on the game, the more influence you will get, and game producers will not be affected by this change, they can freely change the game, merge or shut down the servers.

The change of promotion model: The promotion model of game will be more from advertising bombing, buying and acquiring users to brand promotion and word-of-mouth communication. The game can be promoted at the project stage, showing project goals, obtaining fan support, or “formating of the game community consensus” in the word of blockchain, and then seek users support of game community. Because the investment properties of the blockchain game, users loyalty will be higher, consumption ability is stronger, and they have stronger self-propagation properties. Users are both game users, community participants, “shareholders” and community promoters. Once the promotion method of blockchain game is recognized and accepted by mainstream market, then the knock-off game will be more difficult to obtain living space because one user will not participate in two of the same gaming communities, and it will further encourage game developers to innovate in every aspect.
BlaCat offers an easy to use gaming platform DApp

**Wallet:** Embedded wallet for games covers PC, Android, iOS, Web and other mainstream platforms, facilitating one-click access to games, providing functions such as token recharge, redemption, and virtual item management.

**Games:** As a blockchain game platform, providing game list, recommendations, comments and other functions, similar to Steam, Taptap in blockchain game industry.

**Market place:** To create decentralized tokens, virtual props, and equity trading markets. Through continuous improvement of trading rules, games in community can better realize equity distribution and asset appreciation.

**Community:** A communication platform between developers and users, a channel for promoting games, a decentralized autonomous game community, and autonomous rules and standards.
The introduction of BlaCat

The features description of Blacat project

To meet the business needs of developers: Solving two main business needs of developers, investment and user issues. Solving user traffic problems through a two-level agent promotion system, and solving the problem of developer funds by token holding users to invest in games.

Making users to buy the token easier: BlaCat embedded wallet provides a complete set of recharge system, allowing users to directly convert other mainstream digital currencies into circulation tokens in BlaCat platform. In some specified regions, legal currency channel is directly open, which greatly help users get the token more easier.

Making the transaction speed more faster: Solving the DApp's responding speed to on chain operations, ZoroChain offers a comprehensive blockchain technology solution for high-speed DApp development, including parallel application chain groups for easy expansion, and rich middleware based. The template allows each DApp to quickly link to the public chain based on an independent and efficient parallel application for asset release, and the assets between the parallel application chain and the public chain can be exchanged and circulated.
Make the accessing speed to blockchain faster for developers: BlaCat will provide convenient open source development kit tools that enable traditional game developers to quickly access BlaCat at all levels. This development kit includes various types of game templates for accessing to blockchain, for novice developers, even they do not need to know the lockchain technology.

Solving the high cost problem of developers: BlaCat will also build a fully open source gaming community that will organize community forces to maintain various types of high quality open source game project frameworks, to promote the development of the entire game ecosystem, allowing more game developers to share the progress of the entire community, get avoid of repetitive development, they can develop more quality games easily.

More reliable investment opportunities for token holders: BlaCat will build a mature game rating system based on the community, provide a displaying platform and fundraising channel for projects that need to raise funds, and provide project sources and community rating references for token holders with investment needs.

Embedded wallet

BlaCat offers an embedded light wallet for gamers with following features

**Cross Platform:** Web, PC, Android, iOS are well supported, users can use on various platforms freely.

**Embedded:** Various DApps can easily embed the wallet into the app, making it easy to initiate transactions within the app (Like a cross-platform embedded MetaMask)

**Payment Interface:** Providing payment interface and SDK for common development languages, games developed based on various platforms and various technologies can be easily integrated.
**Virtual Asset Management**: Providing non-homogeneous token management, allowing users to easily manage virtual assets owned by each chain.

Game platform

BlaCat will create a decentralized blockchain game platform like Steam, Tappap, where users can comment, share, and recommend games. Unlike the centralized game platform, all games and content presentations on BlaCat game platform will be decided by on chain algorithm.
BlaCat game platform have following features

Data disclosure: The key data indications of game, such as the number of registered users, the number of active users, the number of paid users, transaction data, and other data reflecting the fundamentals of the game will be disclosed in real time.

**Developer Certification:** Game developers have a certification mechanism similar to Steam Green Light concept. Developers can choose to publicize the information of team and its members, various abilities and qualifications of the company, help users identify the game, and help developers to receive the good public praise.

**Game version progress announcement:** A series of iterative processes, such as historical development process, current version, and future development plans, will be publicly displayed and subject to supervision of community users.

**Comment and score:** Users can comment, score on the game. There will be weighting algorithms (such as the length of game trial, the amount of spending in the game, etc.), high-quality comments, strategy and other articles help users to accumulate community contributions.

**User weighting algorithm:** For users, we will conduct statistics on active behaviors, consumption behaviors, community contributions, etc., and record them to the user's account, which is used to conduct a comprehensive evaluation and rating of the user, and its rating will affect the weight of the user's scoring behavior. Prevent robots and bots from brushing comments to ensure the validity and authenticity of platform users.
**KOL**: For users who have a certain influence in the game field, higher attention will make their high-quality articles, content, etc. get more exposure in BlaCat (based on push algorithm), and the KOL who have accumulated enough attention, also an important part of the game community.

**Smart recommendation**: Combine with game behavior, interested sections, scoring behavior and other comprehensive data to analyze user behavior, and further recommend content to users through fair and open intelligent algorithms.

**Exchange**

BlaCat will further expand and enrich the standards of various types of tokens, virtual assets and equity based on the mainstream blockchain asset standards (such as NFT standards, token standards, etc.) and provide a set of decentralization based on these standards. Trading framework allows the trading market to be quickly implemented based on the framework, while non-gaming users can also trade assets of various games based on the BlaCat platform.
BlaCat exchange have following features:

**Algorithm bank**: A smart contract-based algorithm like Bancor's principle, issuing token like the bank, help game developers to release tokens and anchor the value.

**Smart market maker**: In non-secondary market, users can directly deal with the market maker of the primary market, which is bound by smart contract, and negotiates the trading rules in a programmatic manner to avoid malicious speculation.

**Virtual asset trading**: Users can resell or auction the acquired game assets (virtual items, etc.), like 5173, OPSkin.

**Game token trading**: Indirect token transaction between users and intermediate intelligent market makers, Token price fluctuation is determined by marketing fundamentals.

**Presale**: Developers can launch pre-sales, crowdfunding. Pre-sales and crowdfunding of upcoming online games through smart contract constraints, with agreed return mechanisms.

**Social**

BlaCat offers a decentralized social platform where users can make friends, join the community, share games, play against, and show themselves.

Social on Blacat platform have following features

**Friends**: Follow\Fans (like Weibo) and follow each other to become friends.
**P2P chat:** P2P connection, the transmission of chatting data will be encrypted and these data will be locally encrypted and stored, distributing encryption upload function is provided subsequently.

**News feed:** Users can share their game behaviors, game experience and etc.

**Show:** Users can show their own game achievements, assets, photos, videos and other self-display contents.

**Make friends:** Providing conditional matching, finding someone nearby, team battle and other dating function modules, game developers can freely dock and extend the functions of friends communication and making friends with strangers.