RANGERS

PROTOCOL

Rangers Protocol White Paper

Jan. 2025

WEB3 ENGINE INFRASTRUCTURE

https://linktr.ee/rangersprotocol

White Paper

Table of Content

Introduction	3
About Rangers Protocol	6
Ecosystem Architecture	8
Technical Features	10
Technical Architecture	14
Case Study	21
Token Design	32
Ecosystem Construction	37
Governance Mechanism	39
Token Design, Ecosystem Construction & Governance	49
Mechanism Summary	49
Team, Partners & Investors	50
Roadmap	54
Media	56

01. White Paper
Introduction

01.1 Preface

Rangers Protocol is the backbone of a Web3 Engine for creating immersive Web3 applications. It provides comprehensive infrastructures for complex blockchain-application development, efficient Ethereum-compatible smart contract deployment, ultimate NFT cross-chain interoperability, and developer-friendly IDEs. Through building strategic partnerships in relevant industries, Rangers Protocol supports blockchain entrepreneurs to succeed in the Web3 world. Rangers Protocol minimizes the development difficulty for Web3 developers and maximizes the user experience of its Web3 applications.

For this purpose, Rangers Protocol was founded by a group of senior technical engineers. It took three years to develop an underlying technical solution with a clear framework and functions. Rangers Protocol can provide developers and mass users with simple operation, high security, high performance, high applicability, and high scalability.

From a technical point of view, Rangers Protocol currently has two main components: Rangers Mainnet and Rangers Connector.

Rangers Mainnet is the core sector of Rangers Protocol. It is a high-performance chain that supports complex applications and is highly scalable. It includes:

- the RPoS-based VRF+BLS consensus mechanism;
- the EVM-compatible virtual machine REVM;
- the NFT protocol that can contain historical data of the entire NFT life cycle;
- the storage module responsible for asset and data storage;
- the node module responsible for block generation.

Rangers Connector is a heterogeneous cross-chain solution. It removes the cross-chain communication barriers and lowers the operation difficulty for developers and mass users. It includes:

- a consensus mechanism based on VRF+TSS;
- full nodes of the origin and target chains responsible for providing trusted data services;
- modules responsible for cross-chain transactions.

This white paper holistically describes the design philosophy, methodology, and core technology of Rangers Protocol and explains the specific implementation. It uses simple and readable language to convey information as much as possible. Rangers Protocol strives to enable readers of this white paper to master Rangers Protocol essentials in no time. In addition to the current piece, Rangers Protocol will provide independent yellow papers, developer documents, and other learning materials to elaborate on the diverse features of Rangers Protocol.

01.2 Dictionary

Before reading this white paper, we hope you can spend a few minutes to understand the definitions of the following nouns so that you can read the rest of the piece more easily:

Distributed signature: A cryptographic signature technology based on TSS (Threshold Signature) applied to distributed systems.

Robustness: Refers to the computer system's ability to handle errors during execution and the ability of the algorithm to continue regular operation when encountering input, operation, and other abnormalities.

Contract-level interoperability: The behavior of calling each other's smart contracts between two or more blockchains that support smart contracts.

Blockchain group: A blockchain cluster managed, connected, and formed through Rangers Protocol by multiple isomorphic sub-chains.

Data heterogeneity: Data in different structures.

Horizontal expansion: The ability to connect multiple software or hardware features so that multiple servers can be viewed as one entity.

Zero-knowledge proof: There is an interaction between the prover and the verifier. The prover can convince the verifier that a specific assertion is correct without providing helpful information to the verifier.

RPC: Remote Procedure Call is a computer communication protocol. This protocol allows a process running on one computer to call a sub-process of another computer without the programmer needing to program this interaction.

EVM: The full name is Ethereum Virtual Machine. It is a state transition engine on Ethereum, responsible for the deployment and invocation of smart contracts.

01.3 Abstract

This white paper describes an Ethereum-compatible, distributed-signature-technology based blockchain infrastructure that supports the creation of complex decentralized applications. Although many blockchain infrastructures also provide partial solutions, they do not have characteristics such as robustness, compatibility, and ease of use.

Moreover, they often regard the replacement of Ethereum as the infrastructure of decentralized finance as their primary goal, rather than devoting themselves to building an Ethe- reum-compatible, complex-application-friendly infrastructure.

01.4 Industry Demands

The Bitcoin white paper proposes a peer-to-peer electronic cash system without intermediates. In the past 12 years, more people have realized the value of its underlying technology and recognized it as the next paradigm shift.

Ethereum has gone a step further by launching smart contracts and a decentralized application platform. By providing an infrastructure with a built-in Turing complete programming language, anyone can create smart contracts and decentralized applications in a permissionless manner. Ethereum's mission has attracted world-class developers and formed a global community around it. Nonetheless, the world's population cannot live in one city. In line with the outstanding achievements of Ethereum, it has begun to fail to meet the increasing demand for decentralized applications gradually. This flaw became apparent for the first time when digital collectibles and games blocked the Ethereum network in 2017. Since then, whenever a new popular application appears on Ethereum, the network congestion problem will also occur as if scheduled. The DeFi (Decentralized Finance) boom in mid-2020 and the later bull market have made the congestion problem of Ethereum extremely prominent. The gas price has soared to a record high. The users are getting exhausted when interacting with dapps on Ethereum.

In addition to the above heavy load, when Ethereum was founded, three types of applications were envisaged to be supported: financial, semi-financial, and completely non-financial applications. And imagine the Ethereum protocols should go further than pure currency. The protocols and decentralized applications built around decentralized storage, computing, prediction markets, and dozens of similar concepts should potentially improve the computing industry's efficiency fundamentally. Eventually, there should be a large number of applications that have nothing to do with money. The creators believe that Ethereum is exceptionally suitable as a fundamental layer to serve the vast number of financial and non-financial protocols that will appear in the coming years. However, five years have passed, and people have not seen DeFi-style success in non-financial applications. The digital collectibles and gaming applications that first triggered the congestion problem can only be counted as a minority in the blockchain world.

Over the past few years, with the emergence of phenomenal gaming applications such as Decentraland and Sandbox and pioneering ecosystems such as Web3 Foundation, Metaverse and Web3 have attained increasing buzz and attention in the blockchain industry and communities. Gartner has successfully distinguished the two seemingly homogenous concepts. "Metaverse denotes an evolving vision of a digitally native world in which we will spend our time working, socializing and engaging in all types of activities. " while "Web3 provides decentralized protocols and a technology stack that can be used to build parts of a metaverse and the new communities and economies that it will enable." It makes more sense to perceive Web3 at a technical level while Metaverse at an application level. Always a blockchain trailblazer and always attentive to actual developer needs, Rangers Protocol thus become the first to define and gear toward a Web3 Engine — A Web3 Engine provides decentralized infrastructures, data management, standardized IDEs, and comprehensive interoperability which enable the efficient dApp development in a particular industry.

Rangers Protocol is committed to power a Web3 engine for creating immersive Web3 applications. Suppose Ethereum has built a financial center like New York City. In that case, Rangers Protocol's vision is to create an entertainment and cultural center like Orlando. A new 24/7 entertainment and cultural city is a brand-new virtual world integrated with rich application scenarios such as digital identities, digital assets,

instant messaging, social networks, autonomous communities, interactive games, audio, and video entertainment. Compared with standard financial applications, these atypical scenarios have new high-frequency interactivity, data heterogeneity, and diversity characteristics.

Rangers Protocol integrates cross-chain, NFT, EVM, and distributed network protocols and expands on this basis. It can realize multi-chain contract-level interoperability in the EVM system and scale into a high-performance chain group. In short, Rangers Protocol solves the problem of high-frequency transactions through an efficient VRF+BLS consensus mechanism and the problem of data heterogeneity through a cross-chain solution based on the distributed signature. We also solve the diversity problem through horizontal expansion and the interaction problem through real-time transaction confirmation. It allows developers to freely create decentralized applications that adapt to various scenarios while giving users an Internet application-like experience.

At the same time, just as currency agreements are an essential basis for financial activities, NFT (Non-Fungible Token) is a crucial basis for semi-financial and non-financial actions. Therefore, Rangers Protocol Foundation will also initiate an NFT protocol plan to help more NFT protocols build on Ethereum's basic capabilities and Rangers Protocol to better support the future Web3 standard protocol.

02. About Rangers Protocol

Rangers Protocol is a Web3 Engine infrastructure fully compatible with Ethereum and natively supports NFT and complex applications.

Rangers Protocol integrates and expands cross-chain protocols, NFT protocols, EVM protocols, and distributed network protocols to achieve a high-performance chain group with multi-chain contract-level interoperability in the EVM system.

Instant On-Chain Transactions

Rangers Mainnet adopts an efficient VRF+BLS consensus mechanism to solve high-frequency trading and high-power consumption. It generates truly random numbers at the millisecond, minimizes network congestion, and reduces usage costs for developers and mass users.

Secure Cross-Chain Transport

Rangers Connector utilizes an innovative VRF+TSS consensus mechanism to provide cross-chain services and complete the interconnection with various public chains. It solves the synchronization problem of heterogeneous data sources, transfers assets and data between chains with decentralized security, and enables high-speed network value and information circulation for developers and mass users.

Rich Development Applicability

Rangers REVM is fully compatible with Ethereum's virtual machine but is more functional. It provides comprehensive tool sets to support smart contract development, compilation, and deployment. And it offers custom one-sentence keywords for developers to deploy cross-chain and NFT protocols at ease.

Ultimate NFT Scalability

Rangers Protocol's NFT protocol incorporates ERC-721 to standardize NFT for digital assets. It extends NFT features, including life cycle management, a new data structure supporting data reuse and data rights management based on Dapp latitude; It also innovates cross-chain NFT shuttle, NFT data monitor, NFT rental and collective NFT cross chain.

Rangers Mainnet has integrated an efficient VRF+BLS consensus mechanism to solve the problem of high-frequency trading. Rangers Mainnet produces a block every 1 second. Compared with the traditional PoW production counting in minutes, the efficiency is increased hundreds of times. Furthermore, this efficient consensus algorithm reduces the possibility of network congestion and reduces usage costs.

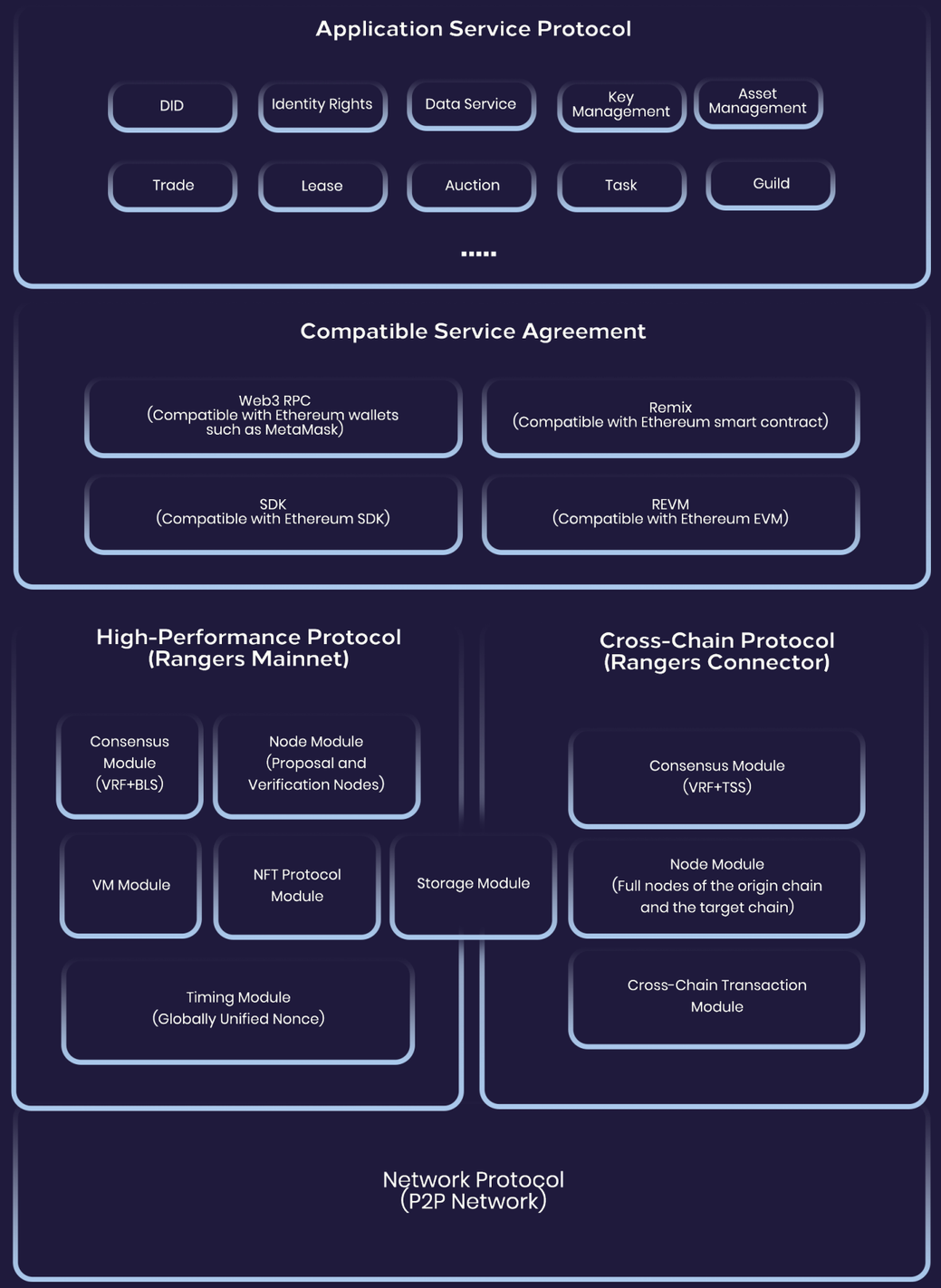
Rangers Connector is a cross-chain solution based on distributed signatures to solve asset migration problems. One of Rangers Connector's visions is to become the bridge for blockchain assets' circulation and connect various public chains. As a result, digital assets will run smoothly between Rangers Protocol and public chains based on the concept of decentralization. For assets that pass through Rangers Protocol – whether they are public chain assets locked to Rangers Protocol or Rangers Protocol assets transferred to other public chains – Rangers Connector has adopted a distributed signature-based consensus system and smart contracts deployed on public chains that verify distributed signatures to ensure the safety of users' assets.

Besides, Rangers Protocol integrated a real-time confirmation mechanism to solve interaction efficiency problems. In Ethereum, due to the uncertainty of the account status caused by the soft fork mechanism, developers often need to decide which account status is the final state based on experience. For example, the common standard requires waiting for six blocks to be generated before providing confirmation. Also, under this asynchronous/waiting mechanism, dapp developers often cannot obtain confirmation in time to process business logic. Conversely, Rangers Protocol can return the execution results in real-time for most transactions without users having to wait for the block to be generated. Rangers Protocol provides a synchronization mechanism for developers that is easy to understand and use.

Rangers Protocol's NFT protocol incorporates ERC-721 to standardize NFT for digital assets. It extends NFT features, including life cycle management, a new data structure supporting data reuse and data rights management based on Dapp latitude; It also innovates cross-chain NFT shuttle, NFT data monitor, NFT rental and collective NFT cross chain.

By integrating various underlying technologies, we have developed Rangers Protocol into an infrastructure that can incorporate financial, semi-financial, and even non-financial dapps.

03. Ecosystem Architecture



Generally speaking, the ecological architecture of Rangers Protocol can be summarized into five layers, namely:

· Application service: Includes identity, rights, data services, key management, asset management, transactions, shops, guilds, lends, auctions, tasks, achievements.

· Compatibility service: Web3 RPC — Remote Procedure Call (compatible with MetaMask), Remix (compatible with Ethereum contract), SDK — Standard Development Kit (compatible with Ethereum SDK), REVM — Rangers Ethereum Virtual Machine (compatible with Ethereum EVM).

· Cross-chain protocol (Rangers Connector): Consensus module (VRF+TSS), node module (full node of the origin chain and target chain), cross-chain transaction module;

· High-performance protocol (Rangers Mainnet): consensus module (VRF+BLS), node module (proposal and verification node), VM module, NFT protocol module, storage module;

· Network protocol (p2p Network): timing module (globally unified nonce), synchronization module (responsive).

04. Technical Features

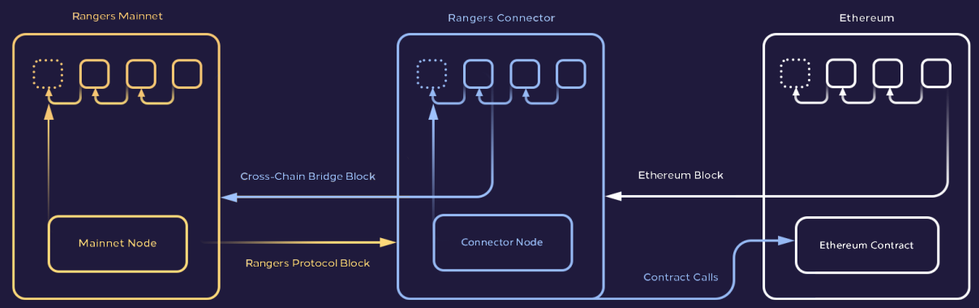
a. Composability and Interoperability

i. Bridging and Cross-Chain Technology

One of Rangers Connector's visions is to become the bridge for blockchain assets' circulation and connect with various public chains. Thus, digital assets can operate smoothly between Rangers Protocol and the public chain based on the concept of decentralization.

For assets that pass through Rangers Protocol – whether they are public chain assets locked to Rangers Protocol or Rangers Protocol assets transferred to other public chains – Rangers Connector has adopted a distributed signature-based consensus system and smart contracts deployed on public chains that verify distributed signatures to ensure the safety of users' assets.

Rangers Connector has proposed a complete set of cross-chain protocols. The cross-chain architecture of Rangers Connector is shown in the following scheme. Rangers Connector node is the primary generating node of the cross-chain bridge. In contrast, Rangers Mainnet node and nodes of other public chains, such as Ethereum, are the actual bearers of cross-chain data.



Taking the NFT assets of the Ethereum ERC721 protocol as an example, the Rangers Connector implementation scheme is as follows:

1. Ethereum assets to Rangers Protocol

- Users send NFT assets-locked transactions to lock the Ethereum NFT assets to a specific contract;
- The Ethereum public chain packs these transactions into blocks;
- Rangers Connector nodes receive the public chain block through the P2P network and parse the public chain asset data. The relevant data will be formatted according to the cross-chain protocol to generate a cross-chain transaction if the asset data is correct;

- Rangers Connector nodes produce a block according to the cross-chain bridge consensus and pack cross-chain transactions when the block is generated;
- Rangers Mainnet nodes receive the cross-chain bridge blocks and verify them according to the cross-chain bridge consensus algorithm;
- After the verification is complete and correct, Ethereum assets are stored in Rangers Protocol. The process of public chain assets transferring to Rangers Protocol is completed.

2. Rangers Protocol assets to Ethereum

- The user submits a transaction application to Rangers Mainnet for the NFT to be listed on Ethereum. The application contains the NFT to be added to the blockchain and the corresponding blockchain address;
- After the Rangers Mainnet node verifies the user's NFT assets, it will be locked. At the same time, package the transaction into a block;
- Rangers Connector node receives the block information from Rangers Mainnet. After checking the block, it extracts all transactions in the block. If there is a cross-chain transaction, the corresponding data is parsed, and a cross-chain transaction is generated;
- Rangers Connector nodes produce a block according to the cross-chain bridge consensus and pack cross-chain transactions when the block is generated;
- Rangers Connector node calls the contract through the Ethereum SDK;
- After the Ethereum contract verifies a distributed signature, it writes the user's NFT data into the contract. The process of transferring Rangers Protocol NFT assets to the public chain is completed.

ii. NFT Protocol

NFT is the foundation of digital assets. In Ethereum, NFT standards such as ERC-721 and ERC-998 are mainly used. Rangers Protocol draws on the advantages of the Ethereum standards mentioned above while expanding its features:

1. Rangers Protocol records the life cycle data of NFTs, including the following stages: NFT Set release, NFT minting, NFT transaction, NFT destruction, NFT transactions to other public chains.

2. In Rangers Protocol, we believe that the most critical value of NFT is reflected in the reuse and inheritance of data. In other words, NFT should be reusable by multiple dapps. To this end, Rangers Protocol expands the NFT protocol as follows:

- Within a specific time, NFT belongs to one particular dapp;
- Each dapp has its own independent data space in NFTs. For all dapps, all data spaces are readable. However, only the currently attributed dapp can modify the data corresponding to this dapp;
- In Rangers Protocol, we have designed the NFT shuttle mechanism so that NFTs can belong to another dapp. The specific process is: the user makes a shuttle request, the current dapp approves it, and the target dapp agrees to receive it;
- We have also designed the NFT lending mechanism. Like renting a house in real life, the renter of NFT only has the right to use it, but not the right to trade.

b. High Performance, High Security, High Stability, And Truly Random Numbers

In the blockchain world, the importance of truly random numbers is self-evident. Generally speaking, a valid, truly random number needs to have the following two characteristics: unpredictability and verifiability. Taking Bitcoin as an example, it uses hash to generate truly random numbers. However, its energy consumption is too large and time-consuming to be used on a large scale. In Rangers Protocol, we combine VRF+BLS technology to generate truly random numbers at the millisecond level.

VRF, or Verifiable Random Function, is the core algorithm Rangers Protocol used to calculate truly random numbers. VRF's input value is combined by the previous random number (the first one is given by the agreement) and some variables representing the height and rounds. Then the private key is used for signing the combination (or, first sign and then combine). Finally, the latest random number is obtained through the hash function. The random number generated can easily be verified by the zero-knowledge proof based on the producer's public key. Thus, it can be seen that VRF contains a total of four functions: 1. Key pair generating function to generate a public key and private key pair; 2. Random number generating function; 3. Zero-knowledge proof-calculating function; 4. Random number verifying function.

In Rangers Mainnet, the random number generation process is as follows:

1. We divide Rangers Protocol nodes into proposal nodes and verification nodes. Proposal nodes are responsible for providing candidate blocks. Verification nodes are randomly divided into a group of 50 nodes, called the verification group;
2. The members of the verification group are mainly responsible for verifying the candidate blocks. First, if the candidate block is legit, the random number fragment is calculated through the VRF function. The input parameters are the member's private key and the random number of the previous block. Then, members broadcast the random number fragments in the verification group;;
3. After the group members receive the threshold number of random number fragments, a complete, truly random number is aggregated and written into the block according to the BLS algorithm. The block is broadcasted to the outside of the group;
4. After the members outside the group receive the block, they can verify the random number's authenticity by calculating the zero-knowledge proof through the group's public key of the group that has been disclosed.

Rangers Mainnet uses the combination of BLS and VRF to allow nodes to cooperate and improve the truly random number system's stability and security.

C. Temporality

Due to the uncertainty of the account status caused by the soft fork mechanism in the traditional public chains, developers often need to decide which account status is the final state based on experience. For example, the common Ethereum/ Bitcoin standard requires waiting for six blocks to be generated before providing confirmation. Also, under this asynchronous/waiting mechanism, dapp developers often need to call back/poll/subscribe to messages to process business logic,

contrary to traditional developers' habits.

In Rangers Protocol, we introduce a global nonce for the transactions sent by users. Rangers Protocol determines the order of transaction execution according to the nonce. Under this mechanism, Rangers Protocol can return the execution result in real-time for most transactions without users waiting for the block to be generated. Rangers Protocol provides a synchronous mechanism for developers that is easy to understand and use.

d. Compatibility: Compatible With Ethereum Virtual Machine

Rangers Protocol is fully compatible with Ethereum Virtual Machine. We want to make it easy for existing and new projects to deploy applications to Rangers Protocol. Most of the currently deployed applications with a decent amount of users are on Ethereum. So it is essential for us to work hard to make Rangers Protocol's operating environment compatible with Ethereum.

We believe that application-level compatibility includes two aspects:

1. Code compatibility;
2. Data compatibility.

Code compatibility means that current developers do not need to obtain new programming knowledge. Instead, they can use existing codebases, including existing smart contracts and front-end application codes, to deploy applications on Rangers Protocol with minimal or no changes.

Data compatibility means that the data in the contract already running on Ethereum, digital assets such as ERC20 and ERC-721, can migrate to Rangers Protocol. This part of the work is already completed through Rangers Protocol's cross-chain solution Rangers Connector.

Ethereum's code compatibility job includes the following aspects:

1. Web3 RPC

A series of modules, including Web3 RPC, has been deployed on Rangers Protocol. The existing tools and applications use Web3 RPC to interact with Rangers Protocol the same way as with Ethereum. From their point of view, it is just connected to another Ethereum network. But, of course, Rangers Protocol also provides many modules that simulate Ethereum components, including blocks, receipts, logs, and the ability to subscribe to log events.

2. MetaMask

Rangers Protocol is fully compatible with Ethereum's applications, services, and middleware. That is, it provides an access mechanism compatible with Ethereum at the level of establishing node connections. For example, because MetaMask holds a dialogue with Web3 RPC or API on Rangers Protocol node, and the MetaMask connection is based on a similar Ethereum function, it is possible to reconfigure MetaMask in a way similar to Ethereum. That is, in the settings of MetaMask, you can access a node based on Rangers Protocol by adding a new network. This mechanism is also applicable to other applications and services of Ethereum. They can either directly communicate with Rangers Protocol through MetaMask or interact with Rangers Protocol in the same way they interact with Ethereum.

3. EVM

Rangers Protocol can fully implement the functions of EVM, and even its key to sign transactions is consistent with that of Ethereum. Firstly, Rangers Protocol is fully compatible with Ethereum's EVM through its REVM: the original contract on Ethereum can be directly migrated to Rangers Protocol for use without recompiling. Secondly, REVM introduces the keywords customized by Rangers Protocol and realizes Rangers Protocol's functions such as cross-chain and NFT protocol with one sentence.

4. Remix

The Remix is a trendy development tool for creating smart contracts and deploying them on Ethereum. Like MetaMask, Remix can connect to Rangers Protocol nodes and be used for smart contract development and deployment.

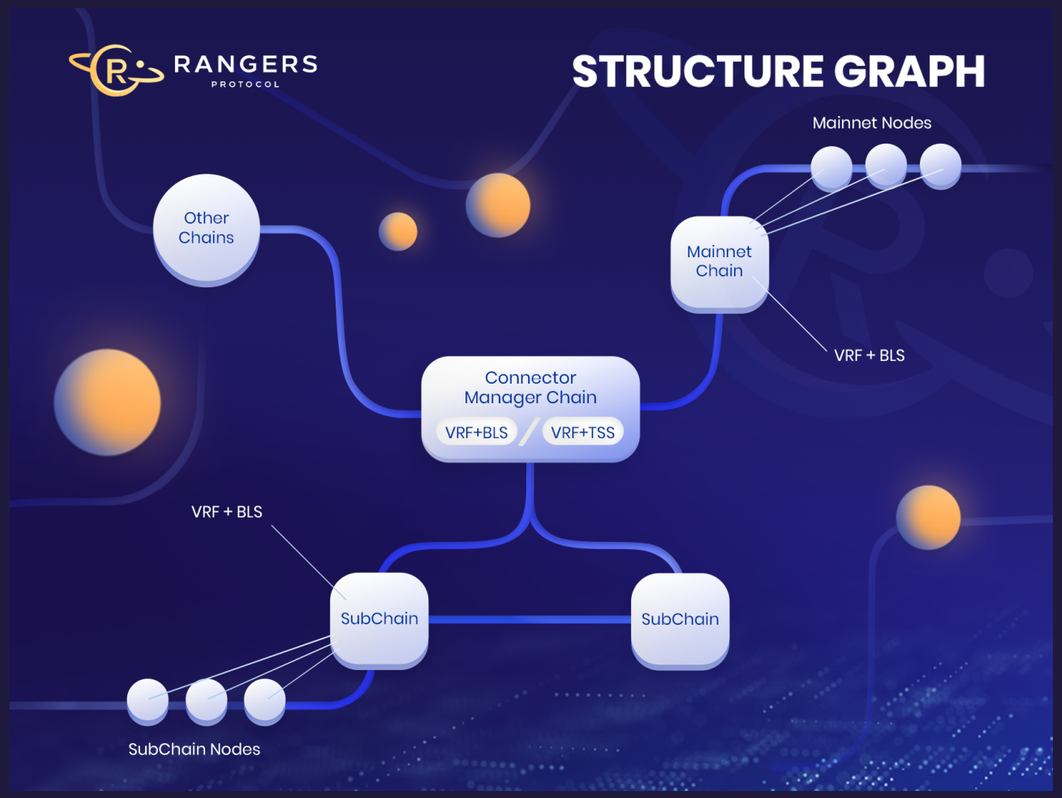
5. SDK

Rangers Protocol SDK is created to comply with Ethereum SDK gateway, which ensures the minimum migration cost for dapps. Rangers Protocol implements JS and Java versions, corresponding to front-end and server-side development, respectively.

e. Ease of Use

While compatible with EVM, Rangers Protocol has created new smart contract keywords for operations such as cross-chain and NFT protocols. As a result, developers who use these keywords in smart contracts can enjoy the unique composability and operability brought by Rangers Protocol.

05. Technical Architecture



a. System Introduction

i. P2P Network

As the basic network architecture, P2P Network supports the data transmission of Rangers Protocol.

This data includes but is not limited to:

1. Transaction data sent by the users;
2. Data related to block consensus, including candidate block data and verification signature data;
3. Data needed by the generation of verification groups, including notification of the generated verification group and signatures of the verification group;
4. Notifications issued by Rangers Protocol include receipts of transaction execution and event data in VM.

ii. Rangers Mainnet

Rangers Mainnet is the core component of Rangers Protocol, mainly composed of the following modules:

1. The consensus module is responsible for implementing the consensus mechanism of BLS+VRF and completing the block generation;
2. VM module is responsible for the execution of smart contracts and the calculation of gas costs;
3. NFT protocol module is responsible for realizing Rangers Protocol's NFT protocol, including NFT merger protocol, NFT shuttle protocol, and NFT data isolation protocol;
4. The storage module is responsible for:

- User asset data storage, including balance, FT, and NFT;
- Block data storage;
- Storage of miner-related data, including miner stakes amount and the member information about the verification group.

iii. Rangers Connector

Rangers Connector is responsible for completing the interconnection with other public chains. Rangers Connector node contains three modules:

1. A full client of Ethereum, which serves as an Ethereum blocks verifier and data loader.
2. A full client of Rangers Protocol, which serves as a verifier of Rangers Protocol blocks, ensures the completion of the cross-chain data storage.
3. The consensus module generates blocks of the cross-chain bridge itself, thereby determining the data involved in the cross-chain.

- Full Ethereum Client

This module works according to the following process:

1. Connects to the Ethereum mainnet to obtain the Ethereum final block through P2P;
2. Verifies the legitimacy of the block header based on DAG (Ethereum PoW consensus algorithm);
3. Executes the transactions packaged in the block, updates the data status of the local Ethereum account, and verifies the results of the transaction execution;
4. If the transaction involves cross-chain transactions of FT/NFT assets, the relevant data will be formatted according to the cross-chain protocol to generate cross-chain transactions;
5. Adds the verified blocks to the local Ethereum chain while maintaining the local canonical chain, including fork processing;

6. Packs cross-chain transactions into the local transaction pool of Rangers Connector.

- Full Rangers Mainnet Client

Similar to the Ethereum full client module, this module works according to the following process:

1. Connects to Rangers Mainnet to obtain Rangers Mainnet blocks through P2P;
2. Verifies the legitimacy of the block header based on VRF+BLS (Rangers Mainnet Consensus Algorithm);
3. Executes the transactions packaged in the block, updates the data status of the local Rangers Mainnet account, and verifies the transaction execution results;
4. If the transaction involves cross-chain transactions of FT/NFT assets, the relevant data will be formatted according to the cross-chain protocol to generate cross-chain transactions;
5. Adds the verified blocks to the local Rangers Mainnet chain while maintaining the local canonical chain, including fork processing;
6. Packs cross-chain transactions into the local Rangers Mainnet Connector transaction pool.

- Consensus Module

Similar to Ethereum, the block-producing node is also determined by PoW between Connector nodes.

Block producers will package all cross-chain transactions in the local Rangers Mainnet Connector transaction pool.

The generated blocks will be broadcasted through Connector's P2P network.

b. Consensus Mechanism

i. BLS+VRF

VRF, or Verifiable Random Function, is an algorithm for generating random numbers. The advantage of using VRF is the relatively low power consumption. With the latest algorithms, verifying the legitimacy of VRF has been very fast, and it is an efficient consensus algorithm. In Rangers Mainnet, the VRF algorithm is used to select candidate block packers and candidate block verification groups.

The BLS signature algorithm was proposed by three people from the Department of Computer Science at Stanford University: Dan Boneh, Ben Lynn, and Hovav Shacham. BLS's main idea is to hash the message to be signed to a point on an elliptic curve and use the exchange property of the bilinear mapping E function to verify the signature without revealing the private key. Rangers Mainnet is mainly used to aggregate each member's signature in the verification group for the candidate block to generate the verification group signature.

ii. Verification and Proposal Nodes

Rangers Mainnet adopts a group consensus mechanism based on VRF+BLS technology. Therefore, the grouped nodes need to be divided into two categories – proposal nodes and verification nodes.

The proposal node is responsible for the construction of candidate blocks. The verification nodes are randomly grouped. The verification group confirms the legitimacy of the candidate block by the cooperation of the group members.

C. REVM

Rangers Protocol's REVM is fully compatible with Ethereum's VM. Thus, the original Ethereum contract can directly migrate to Rangers Protocol for use without recompilation. Like the Ethereum development toolchain, Rangers Protocol also provides toolchains such as Remix and MetaMask to support smart contracts' development, compilation, and deployment.

Besides, REVM also introduces Rangers Protocol custom keywords to complete Rangers Protocol features such as cross-chain and NFT protocols with one sentence. Developers who use these keywords in smart contracts can enjoy the unique composability and operability brought by Rangers Protocol. Contracts that use these keywords must be compiled by REVM to generate usable bytecode.

The transfer of the Rangers Protocol smart contract is still based on the transactions and ABI system. In addition, in Rangers Protocol, the gas/gas price required to execute smart contracts can be paid by multiple parties: either the invoker or the contract issuer.

d. Information Upload Process

i. Ingot Process

In each round of Rangers Protocol consensus:

1. We first use the truly random number generated by the VRF algorithm to select the proposal nodes and verification group by drawing. In each proposal round, multiple proposal nodes can propose multiple candidate blocks at the same time, but each candidate block will have a different priority to facilitate the fork process;
2. The proposal node sends the candidate block to the verification group. Each member in the verification group verifies the legitimacy and priority of the candidate block and broadcasts the signature of the verification result in the group;
3. When the number of the signatures collected by the verification group reaches a threshold, the BLS algorithm can recover the verification group signature. The corresponding candidate block wins and is broadcasted to the entire network;

4. All nodes receive the consensus result and verify the group signature through the verification group public key. After the signature is confirmed, the next round of consensus starts.

Rangers Protocol dramatically reduces the possibility of the two teaming up to do evil through the role division mechanism. The VRF algorithm guarantees that the proposal nodes and verification groups are random, unpredictable, unselectable, and unconcealable. From the perspective of communication complexity, signature length, and performance, we believe that the BLS threshold signature algorithm is more robust to be used in the verification groups than the Byzantine fault-tolerant algorithm.

ii. Group Chain Model

VRF consensus algorithms such as Algorand usually select multiple verification nodes in each consensus round to vote for the candidate blocks. For better performance, Rangers Protocol improves consensus efficiency by generating verification groups in advance.

Also, in order to reduce the possibility of the verification group doing evil, each verification group has life cycle control, and it is regularly disbanded and reorganized.

Besides, the verification group members are peer nodes on the decentralized network. Inevitably, the verification nodes may not be online for various reasons at certain moments, such as poor network connection and malicious nodes' deliberate inaction. Therefore, the verification group needs (t, n) threshold signatures, where n is the number of group members, and t is the recovery threshold. Usually, $t \leq n$. If more than t nodes in the group sign the message, the entire group approves the message. Then, the group approval signature of the message can be recovered..

1. Group Inspection

Rangers Protocol conducts the group inspection at a fixed rate. Assuming that the current block height satisfies the fixed-rate condition, the current verification group needs to conduct a group inspection after the block generation. This verification group is called the father group. The father group requires to complete the following tasks:

- Each member in the father group first determines the list of verification nodes according to certain criteria;
- Each member of the father group randomly selects multiple candidate verification nodes from the verification node list through VRF. At the same time, the selected results will be broadcasted in the group;
- Pass the threshold signature consensus in the father group to determine the legitimacy of the selection result;
- The father group members notify the candidate verification nodes to initiate the creation of a new group.

2. Creation of New Groups

Here we use the decentralized Shamir secret sharing algorithm to generate the group signature private key Si of each node, the group signature public key MPKI,

and the group public key GPK corresponding to the group's private key representing the group consensus to obtain the above secret key, and reach an agreement on the group public key GPK, then the group creation is completed. The specific steps are as follows:

- Each team member selects their secret polynomial;
- Each team member calculates the shared secret to other team members and sends the shared secret to the corresponding team members. At the same time, send their own public key PKI to other team members;
- When the team members collect all the shared secrets from other team members, they calculate all the received shared secrets Si and GPK;
- Each group member calculates the group signature public key MPKI corresponding to the signature private key Si in the group and informs the group signature public key MPKI to the other group members.

Note that the communication between the group members in step 2 needs to be encrypted to prevent it from being monitored. Therefore, the common user public key PUBK of all group members is recorded in the miner information. We use this as the ECDH key exchange for encrypted communication. After the above steps, each group member obtains the group signature private key Si, the group signature public key MPKI, and the group public key GPK corresponding to the group private key SK. Because each team member only knows their initial secret SKi, they cannot see the value of SK.

3. Verification Group Signature Mechanism

The verification group signature mechanism mainly uses the BLS algorithm: on the Barreto-Naehrig elliptic curve, after the group member signature private key obtained by the construction method mentioned above signs the message, when the message signatures of the k members in the group are received, the Lagrange interpolation polynomial can be used to obtain the signature of the group private key SK for the message.

In the Shamir secret sharing algorithm, recovering the group's private key SK requires revealing of Si. Using the nature of bilinear mapping, the group private key's signature can be completed without revealing Si, ensuring that the group member's signature private key can be continuously reused. Through this technology, a consensus within the group can be achieved through threshold signatures. The efficiency is higher than that of the Byzantine algorithm (BFT).

Since no one knows the verification group's private key SK, the signature is unselectable, unpredictable, and unchangeable. However, the group public key GPK can be used to verify whether the group provides the signature.

e. Access Process

i. Game Access Process

For developers who use Rangers Protocol to develop blockchain games, the following access process is required:

1. Rangers Protocol blockchain

Build the node yourself, and the terminal will access the built node to obtain data. Or visit the free Rangers Protocol test environment to save the trouble of making nodes.

2. Use WebSocket/SDK to access nodes

After users establish a connection with Rangers Protocol through the standard WebSocket protocol, they can use the JSON RPC API to access Rangers Protocol data, including account information, transactions, and blocks. Rangers Protocol also supports WebSocket to send transactions, compile/deploy and transfer smart contracts, and other functions.

At the same time, Rangers Protocol provides JS/JAVA SDK. They encapsulate the WebSocket of Rangers Protocol and conveniently deliver the functions mentioned above to interact with Rangers Protocol.

ii. Public Chain Access Process

The public chain enters Rangers Protocol mainly to realize the intercommunication of digital assets. The public chain access process is as follows:

1. Deploy Rangers Protocol smart contracts on the public chain

The smart contracts deployed on the public chain are mainly responsible for locking and unlocking public chain assets. Rangers Protocol requires the smart contract system of the public chain to have the following characteristics:

- It is possible to develop smart contracts similar to ERC-20 and ERC721;
- The SECP256 signature algorithm is supported in the contract, which is used to verify Rangers Protocol consensus signature information;
- The contract supports an event mechanism similar to EVM, which can pass locked asset information to Rangers Protocol;

2. Rangers Protocol needs to develop functions related to the public chain, and the public chain needs to provide relevant cooperation.

- The public chain needs to provide the GO language version of the SDK to support Rangers Protocol to transfer the contract deployed on the public chain;
- The public chain offers a method for subscribing to contract EVENT data, and Rangers Protocol can efficiently obtain contract data.

06. Latest Case Study

a. Rocket Protocol 1.0

i. HyperDragons Rocket Arena (2018-2020)

Rocket Protocol 1.0 is a Layer-2 scaling solution based on Ethereum. Combining Layer-2 and Layer-1 smart contracts solves the cost and performance problems of in-game high-frequency state updates while retaining decentralized characteristics. Here are some changes that occurred in HyperDragons Rocket Arena after completing the renovation with Rocket Protocol 1.0:

[Competitions]

To enter the arena, users need to lock the dragon. When the dragon needs to be traded or bred, it needs to be unlocked. This is the meeting point of the two layers' interoperability. After the users complete the competition registration, they lock the dragons in Layer-1 and open them in Layer 2. As long as the users do not unlock the dragon, they can always register for the competition and experience the rich gameplay smoothly. Therefore, from the perspective of a single game, there is one extra lock/unlock operation in the process. However, from the perspective of multiple games, Layer-1 operations have been reduced, saving the users' total cost as a whole.

[Forecasting]

The forecast market is fully realized in Layer-2. Users can immediately see the ratio change, participate in or cancel predictions, and do not have to wait another 5-30 minutes to confirm each operation.

Funds Pool

1. Users now have a Fund Pool in Layer-2, including Layer-1 and Layer-2 cross-chain ETH and ERC20 assets used in high-frequency usage scenarios. Except for recharge and

withdrawal operations (to complete the process of locking/unlocking the Funds Pool), the entire system's operating procedure has not changed much. Many previous Layer-1 operations, such as creating a competition or calculating its results, are now calculated on Layer-2. Calculations have resulted in three significant advantages:

1. Miners' fees saving (total cost)
2. Real-time response (no need to wait for transaction confirmation during each operation)
3. Anti-congestion (Layer-2 part can work efficiently while Ethereum congestion).

b. Rocket Protocol 1.5

i. HyperSnakes (2019-2020)

Based on Rocket Protocol 1.5, HyperSnakes received several upgrades, including:

1. An efficient VRF+BLS consensus mechanism;
2. Proposal and verification nodes, block generation verification (node governance);
3. Multi-chain identities and DID architecture;
4. Bridging and cross-chain.

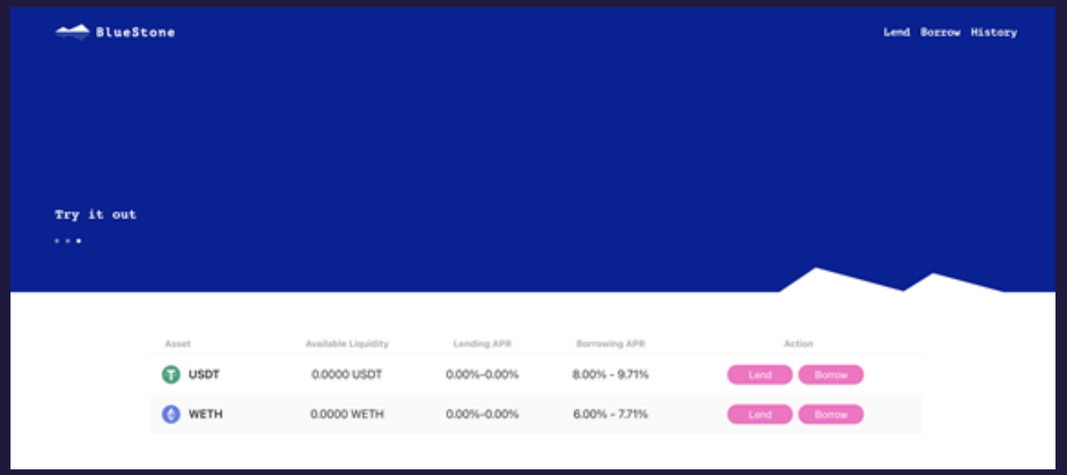
After the launch of Rocket Protocol 1.5, the HyperDragons application was released on ETH, Tron, ONT, and Ant Blockchain almost simultaneously. The Ant Blockchain-based HyperSnakes appeared in the popular section on the Alipay homepage during March 2020. It withstood the extreme test of adding 20,000 new users daily for a week while maintaining robustness and fluency and providing an Internet application-like experience.

C. Rangers Protocol

In June 2021, Rocket Protocol 1.5 was renamed Rangers Protocol and underwent a comprehensive brand upgrade. After a lot of business practices and market research, the team, unfortunately, found that the blockchain industry is still in its early stages. It is not only infrastructure and standard protocols that restrict large-scale multi-person decentralized applications from entering the fast lane of development, but also new business models, wide market acceptance and large-scale migration of user habits, and many other factors. But based on a deep understanding of the business environment and underlying technology, Rangers Protocol quickly focused on professional support for NFT and complex applications::

1. Extensible public link entry scheme, users' existing multiple digital assets can be used in dapps;
2. A mechanism that can shuttle and convert FT and NFT among multiple dapps, helping users efficiently reuse digital assets;
3. Compatible with EVM smart contract system and NFT protocol stack, helping developers to smoothly upgrade dapps;
4. A complete development and operation and maintenance system helps developers to efficiently develop and operate dapps.

i. BlueStone (2021)



Due to Rangers Protocol's full compatibility with Ethereum EVM and high level of integrity with Truffle and MetaMask, the process of porting dapps from Ethereum to Rangers Protocol is highly developer-friendly and smooth, which is mainly reflected in the following aspects:

1. No contract changes required

Since Rangers Protocol is fully compatible with Ethereum EVM, BlueStone, based initially on Ethereum, can be deployed directly to Rangers Protocol without modification.

2. Contract deployment without failure

By running "truffle migrate — network main," developers can deploy dozens of

contracts to the Rangers Protocol main- or testnet, and the process is quite simple. First, the Rangers Protocol network information must be added to truffle-config.js. Rangers Protocol provides JSON-RPC API: https://testnet.rangersprotocol.com/api/jsonrpc, which can be used to start wallet providers. Then the network name specified by truffle-config.js can be used to execute the truffle migrate command to deploy all contracts to Rangers Protocol.

Compared to deploying dapps in Ethereum, the experience on Rangers Protocol is more developer-friendly, which is reflected in lower costs and faster speeds. Unlike the mechanism that requires a higher gas fee specified in Ethereum, Truffle uses the fixed gas fee determined by the developer in truffle-config.js to interact with the network. As Ethereum's gas fee fluctuates wildly, developers must specify a relatively high gas fee in truffle-config.js to ensure that dapp deployment can be completed within a reasonable time frame. However, it is more controversial how high a gas fee needs to be stipulated. The higher the specified gas fee, the more US dollars will be consumed, causing waste. Rangers Protocol eliminates this concern with a fixed fee of 0.0001 RPG per transaction. In addition, the block generation time of Rangers Protocol is faster than that of Ethereum, so the deployment speed on Rangers Protocol is much quicker than that of Ethereum.

3. Minimized front-end changes

Rangers Protocol is highly integrated with MetaMask. Like Ethereum testnet, developers only need to integrate the necessary contract addresses into the front-end code and interact with them when Metamask is in the Rangers Protocol network (Chain ID: 2025).

4. Web3 script

Rangers Protocol's package manager is compatible with Web3. Developers have some maintenance scripts that can use Web3 to interact with Ethereum smart contracts. By importing the Rangers Protocol version of the Web3 software package, the code can remain unchanged.

d. Rangers Protocol Updates

In 2022, to better minimize the development difficulty for Web3 developers and maximize the user experience of its Web3 applications, Rangers Protocol released a batch of tool sets deployed on the Rangers Mainnet and Robin Testnet. The tool sets provide its users with the greatest convenience in using Rangers Protocol for FT and NFT cross-chain, mining, and more Web3 applicational scenarios. The Tools Library is accessible on the Rangers Protocol official website under the Tools tab and it currently includes the following main usage aspects:

1. Rangers Mainnet Tools

There are 4 types of tools deployed on Rangers Mainnet for developers and users. Rangers Connector's cross-chain tools for FT and NFT (upcoming); Rangers Scan for queries on blockchain operations such as on-chain transactions and blockchain generation; Miner Console for miner management through functions such as Miner Apply, Miner Unstake, Miner Change, and Miner Add; and Rangers Claim for investors to claim their RPG (Rangers Protocol Gas) tokens.

2. Robin Testnet Tools

Developers are always welcomed to explore Rangers Protocol's services on Robin Testnet with free RPG test tokens from Rangers Faucet. They can also browse relevant data using Rangers Scan. Services open for developer experience include not only the tools functioning on Rangers Mainnet but also the ones still in the testing phase. For instance, the NFT cross-chain function of Rangers Connector is available for testing.

3. Upcoming Tools

In addition to the above-listed tools that are currently in service, more of them are coming on the way. Light Wallet, a convenient Web3 on-ramp tool, will be the next to meet the users and help them enter the Web3 world through Web2 login methods, free from the complex Web3 process with recovery phrases.

Rangers Protocol aspires to build a Web3 engine for creating immersive Web3 applications. The existing Web3 infrastructures provide developer-friendly solutions for complex-app development, and the upcoming tools and services would further enhance this concept and bring Web3 on-ramping convenience to mass users as well.

07. Rangers Connector

a. Why Do We Develop Cross-Chain?

i. The Need for Cross-chain

With the development of blockchain technology, the industry has witnessed an unprecedented explosion in a short period. Represented by the vigorous development of the new public chain, the rise of ecosystems such as BNB Chain, Solana, Polygon, and Heco marks that we are already in an era of multi-chain. Just as different countries and regions need to establish intermediary agencies to transfer assets and information, it is necessary to develop bridges between various chains to transfer data and assets. Therefore, cross-chain has become the most fundamental need in various interconnecting projects, ecologically communicating among ecosystems and constructing the Metaverse.

Cross-chain mainly solves the problem of barrier-free circulation of data and assets in a complex multi-chain mode. These can be roughly divided into FT (Fungible Token) cross-chain and NFT (Non-fungible Token) cross-chain.

ii. Current Cross-chain Solutions

There are already many solutions for FT cross-chain, such as AnySwap and Rainbow Bridge of NEAR. Although solutions for the NFT cross-chain are also emerging, their technical maturity needs further verification. Many NFT cross-chain solutions share some shortcomings, such as the inability to save block information. There are even solutions that will burn cross-chain NFTs and remint new ones.

In terms of adopting cross-chain technology, relay chain technology is currently a more popular one. The essence of relay chain technology is that the target chain itself verifies whether the message sent by the relay chain belongs to the origin chain. The core of its security is whether a reliable origin chain light client is implemented on the target chain.

NEAR Rainbow Bridge

The downlink channel of ETH <> NEAR Rainbow Bridge monitors and reads each block on ETH for the operation of the coin lock contract. The uplink channel of Rainbow Bridge will push a batch of public keys to the consensus-involved nodes in each cycle through the characteristics of BFT-based sharing. Withdrawal requests verified by the NEAR blockchain block header are reserved for 4 hours of challenge time. If there is no challenge, the withdrawal and transfer will be executed after 4 hours. (It is a bond proposed by the challenger. The challenge request can only be performed after the verification signature of the request from the challenger is passed. If the challenge is successful, half of the bond will be returned. This withdrawal request will not be executed). The cost of this solution is prohibitive because the signature verification function it uses in the challenge phase is not a system function of the Ethereum contract but a function of NEAR itself.

Poly Network

Poly Network's verification block is very similar to that of Rainbow Bridge. Poly also uses BFT's consensus system, which also has cycles. Unlike the Rainbow Bridge, Poly uses the built-in functions of Ethereum, so it does not have the cost problem of the Rainbow Bridge. In addition, Poly adopts the standard multi-signature verification. Therefore, it is a multi-signature solution with a light client (verify block header).

iii. Rangers Connector

Rangers Protocol has designed Rangers Connector to achieve cross-chain functions.

Rangers Protocol believes that security is the top priority in cross-chain solutions. Showing users the security of cross-chain is a problem that needs to be considered for a mature cross-chain solution. As Rangers Protocol's tool to undertake the cross-chain function, Rangers Connector implements cross-chain functions through distributed signature technology and the Secure Multi-Party Computation Chain based on the VRF+TSS consensus mechanism. Based on thoroughly ensuring cross-chain security, it completely preserves cross-chain data.

b. What Is Rangers Connector

i. Overview

Rangers Connector is an essential part of Rangers Protocol, which assumes the responsibility of interconnection with various public chains. It includes:

- A consensus mechanism based on VRF+TSS
- Full nodes of the origin and target chains responsible for providing trusted data services
- The module responsible for cross-chain transactions

ii. Technology Used

VRF

VRF is an algorithm for generating random numbers. Unlike ordinary random algorithms, VRF allows all parties to generate random numbers independently without being manipulated to cheat. It is also used in Rangers Mainnet and works with BLS in the process of block generation. In Rangers Connector, the VRF algorithm selects candidate block packagers and candidate block verification groups.

TSS

TSS is called Threshold Signature Scheme. It is a technology that changes the traditional 1:1 correspondence between the public and private keys to 1:N public and private keys proportion. The algorithm can be passed as long as t of the N private keys are used to sign the message independently. What differentiates it from multi-signature is that the latter occurs on the chain, while the threshold signature occurs off-chain, which can save the cost of calling operations on the chain multiple times.

iii. Technical Solution Analysis

The overall cross-chain solution of Rangers Connector can be divided into two stages:

- Realization of asset and data cross-chain through the distributed signature system;
- Realization of the Secure Multi-Party Computation Chain based on the VRF+TSS consensus mechanism.

The Rangers Connector cross-chain bridge comprises N nodes, and the consensus is reached efficiently through the TSS algorithm. The cross-chain bridge nodes are also the full nodes of the origin and the target chains and will monitor the coin lock event of the origin chain. After the consensus based on TSS is reached, the cross-chain bridge will write the consensus data into the cross-chain information table. Through the interception program of the cross-chain bridge, the NFT contract owner of the target chain can monitor the state change and obtain consensus data, including origin chain NFT contract address, NFT cross-chain request transaction hash in origin chain, target chain type, target chain contract address, and NFT status information. In the end, the NFT contract owner triggers and completes the data migration work of the relevant NFT through the cross-chain information that has been fully agreed upon.

After realizing a secure cross-chain, Rangers Connector will generate a new blockchain called the Secure Multi-Party Computation Chain (SMPCC). The Secure Multi-Party Computation Chain based on the VRF+TSS consensus mechanism is derived from the multi-party computing (MPC) technology. Multi-party computing is a group of mutually distrustful parties attempting to jointly compute a function on their inputs while maintaining the privacy of these inputs. The role played by TSS is that there is only one public key for the threshold signature, but it requires t signatures out of the N private keys to take effect. This signature occurs in SMPCC, and the N private keys are stored separately by its nodes. The VRF can randomly select nodes with the private key to sign and initiate operations on the target chain.

iv. Advantages of Rangers Connector

High Security

Rangers Connector first solves the cross-chain problem from the perspective of consensus. Rangers Connector outputs a consensus that can be verified by other chains, effectively avoiding security issues.

Scalability

The TSS-based distributed signature system uses the same elliptic curve (secp256k1) as mainstream public chains like Ethereum and BNB Chain. This technology can extend the consensus system of Rangers Connector to other public chains, so that it can be verified by the smart contracts of other chains.

Strong Connectivity

Rangers Connector performs cross-chain by outputting consensus, which can

connect various heterogeneous chains. The consensus level will not be compromised in the cross-chain procedure, and the cross-chain data can be saved entirely so that the cross-chain data can be reused on other chains.

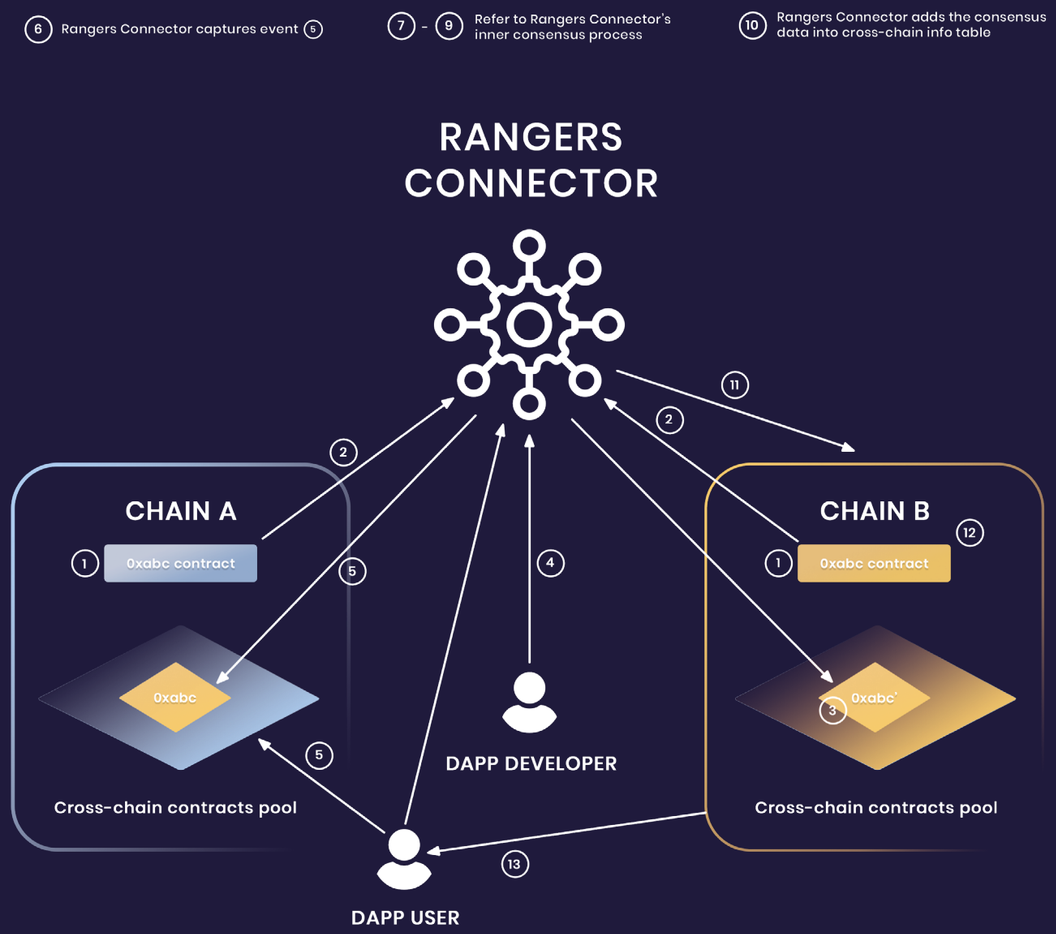
C. Rangers Connector Implementation

i. Cross-Chain Process

The cross chain of Rangers Connector is realized by the cross-chain bridge listening to the origin chain and the target chain. Assets will not be locked in the cross-chain bridge during the cross-chain process. And thanks to the state synchronization mechanism used in the cross-chain process, the historical data of assets can be completely preserved. Taking NFT cross-chain as an example, the detailed cross-chain process is as follows:

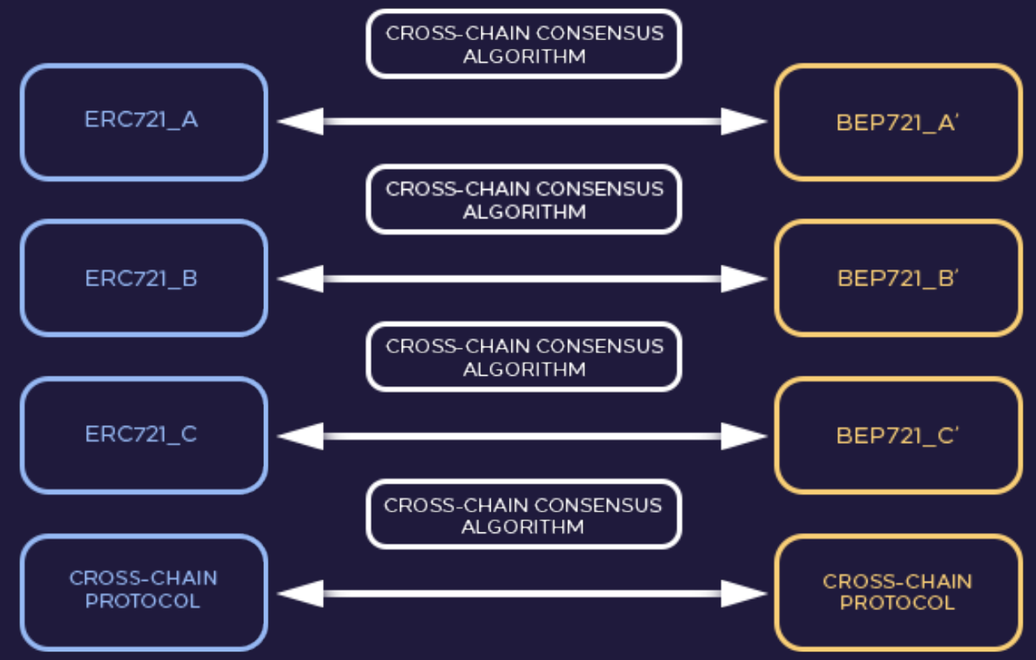
Suppose the origin chain is chain A, the target chain is chain B, and the cross-chain NFT is 0xabc.

1. The dapp developer deploys the NFT contract of 0xabc on chain A and chain B respectively;
2. The dapp developer needs to submit the names of the two chains, the contract addresses, and the NFT project name to Rangers Connector. Rangers Connector sets the above information into the cross-chain system of chain A and chain B and provides the dapp developer with the cross-chain contract address;
3. The dapp developer adds 0xabc's replica 0xabc' into the NFT contract of chain B;
4. The dapp developer locks 0xabc' in the cross-chain contract of chain B;
5. The dapp user initiates a cross-chain request of 0xabc to the cross-chain contract of chain A, and authorizes Rangers Connector to lock 0xabc in the cross-chain contract of chain A;
6. The Rangers Connector nodes detect the lock event;
7. The node that detects the lock event initiates a cross-chain consensus and starts the consensus through TSS-LIB. The node conducts verification and TSS signature first, and then broadcasts to other Rangers Connector nodes;
8. Other nodes decide whether to confirm the cross-chain request based on the information they have detected, and if so, conduct TSS signature;
9. If the number of TSS signatures exceeds the threshold, a consensus is reached;
10. Rangers Connector adds the consensus data into the cross-chain information chart;
11. Rangers Connector sends a consensus-successful cross-chain request to chain B;
12. The NFT contract on chain B verifies the validity and legitimacy of the TSS group signature;
13. Upon a successful verification, chain B transfers 0xabc' from the cross-chain contract to the dapp user, and the cross-chain process is completed.

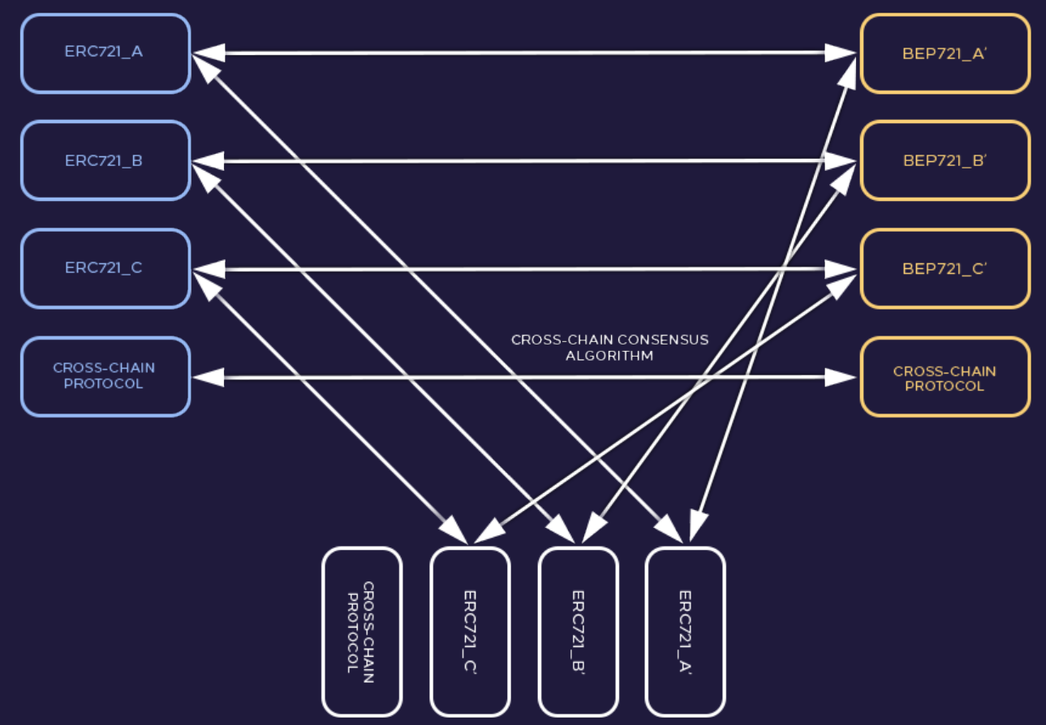


In addition to cross chain between two chains, Rangers Connector also supports simultaneous cross chain of multiple NFT contracts. Additionally, the cross-chain logic between multiple chains is the same as in two chains, and it is also carried out through a cross-chain consensus program.

A. Cross-chain between two chains



B. Cross-chain between multiple chains



iii. Blockchain Explorer

Rangers Connector designs the blockchain explorer Rangers Scan as a cross-chain data query tool. All blockchain operations in Rangers Connector will be recorded on Rangers Scan so that every transaction can be traced.

08. Token Design

a. Token Definition

RPG (Rangers Protocol Gas) is the Rangers Protocol ecosystem token, with a total supply of 21 million pieces. In the economic system of Rangers Protocol, ecological nodes that generate blocks are divided into proposal and verification nodes. This system adopts an open participation mechanism, allowing all users to participate in the system's operation.

b. Design Principles

Technically, Rangers Protocol implements parallel computing through VRF random election + BLS signature algorithm and introduces high-concurrency collaboration and preprocessing technologies in distributed systems. It is better than Bitcoin in terms of decentralization — any device network-compatible can become a node. In terms of security, VRF truly random numbers select groups to ensure that the working group is unique at a certain altitude. The periodic CheckPoint mechanism ensures that the block data is "final." It eliminates problems such as long-range attacks and private mining.

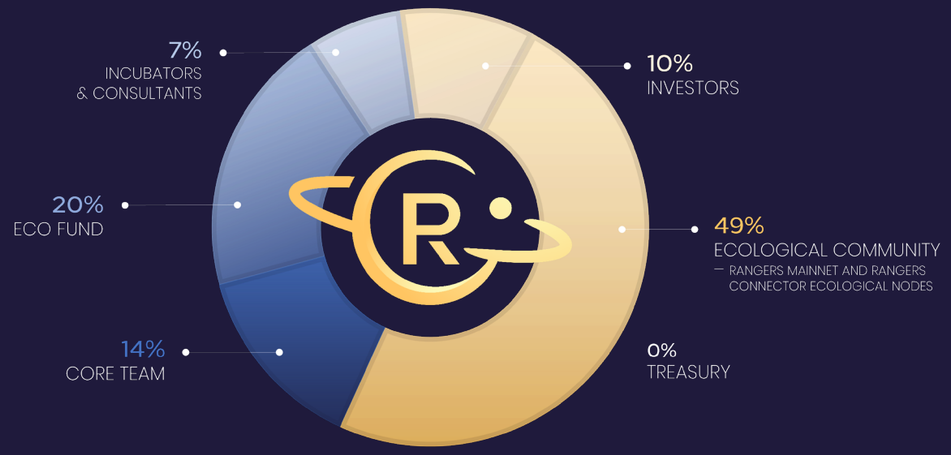
In terms of design, the token economy system must create real value for each user and encourage users to increase their productivity. Therefore, Rangers Protocol designed the Protocol Principle and Transparency Principle. Protocol Principle: an excellent economic system relies on protocol behavior and economic incentives rather than lengthy procedures and coercive measures. Transparency Principle: the system can have a centralized design, but the black box should be eliminated as much as possible.

C. Token Allocation

RPG Economic Circulation

Tokens will circulate among users, developers, investors, and ecological nodes. First, Rangers Protocol will be connected to major platforms and encourage developers to develop, distribute, and operate their applications based on Rangers Protocol. Secondly, Rangers Protocol has designed the tokens purchase and stake mechanism, meaning developers need to purchase and stake tokens to use Rangers Protocol. When users experience or invest in applications that access Rangers Protocol, they also need to buy and consume tokens. For instance, they can pay tokens to application developers. With the ecosystem's expansion, the token will continue to increase in value. More and more token holders and more ecological nodes will make it a virtuous economic cycle.

d. Specific Content



1. Investors (10%): Equal unlock (claim) each day. Token allocation for investors will be fully unlocked within 400 days.
2. The core team (14%): core developers and maintainers, 8% of the remaining amount is released every 180 days
3. Incubators and consultants (7%): Incubators and strategic partners, 8% of the remaining amount is released every 180 days
4. Ecological community (49%): 8% of the remaining amount is released every 180 days, the ecological community consists of ecological nodes of both Rangers Mainnet and Rangers Connector.

- Rangers Mainnet Ecological Nodes (35%)

  Proposal nodes (24.5%): join through RPG-staking election and provide special hardware

  Verification nodes (10.5%): stake RPG, and provide required hardware

- Rangers Connector Ecological Nodes (14%)

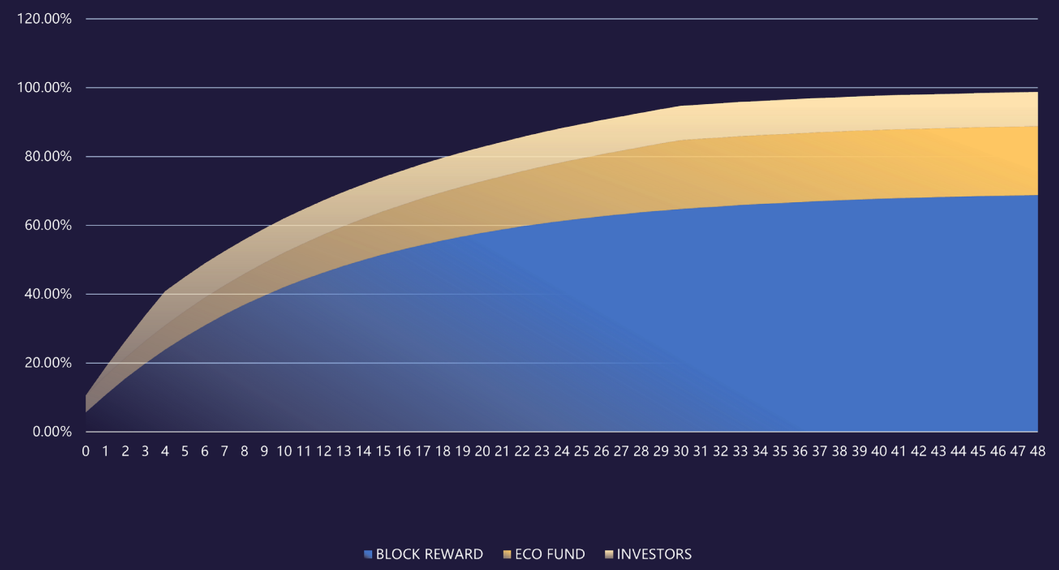
5. Ecological fund (20%): The unused amount is locked, community voting will be held, and relevant announcements made on the foundation website upon use

- Market Operation (8%): DAO mechanism approves proposals based on community voting
- Developers (7%): Grant mechanism distributes rewards to community members based on contribution,
- Market Value Management CEX (2%)
- DEX Liquidity (1%)
- KOL (0.83%)
- Liquidity Rewards (0.67%)
- IDO (0.5%)

6. Treasury (0%): reward and penalty pool, dynamically balanced during operation, the value can be adjusted by community voting

- Slash mechanism: punishment based on the security threat level
- Taxation mechanism: service fees for middle layer protocols and upper-layer applications

e. Supply Mechanism



f. Block Production Process and Incentive Mechanism

i. RPG Block Production Process

1. Nodes that produce blocks will get corresponding rewards. The proposal node (proposal group) sends a proposal and hands it over to the verification node (verification group) for verification. After all individual verifications complete the signature verification, a group signature is formed. The block is allowed to be produced and broadcast.

2. Average block production time: 1 block/second

3. Block-production node designation: Multiple nodes compete to form block nodes according to the established VRF random number.

4. Block generation mechanism: Each time a block is produced, the candidate nodes of the entire network randomly generate multiple proposal nodes through the VRF algorithm so that the proposers are random and unpredictable. The proposals are sent to the verification group in various channels in parallel, which limits the situations where the proposals and verifications misconduct.

The VRF mechanism selects the verification group based on the threshold signature scheme, ensuring that the verification group is unpredictable, unselectable, and unconcealable. When the block is produced, it is only necessary to achieve a lightweight verification within the group. The block is created quickly in a multi-channel parallel pipeline. Soft forks' problem will not arise because the block generation rules directly specify a node to generate blocks. Even if another node completes the proposal simultaneously, it will not be selected as a block-generating node.

ii. Within Block Production Process

1. VRF selects proposal a node from the proposal group and is responsible for generating blocks;
2. The proposal node selects the verification group through VRF, and the proposal node sends the block to each member of the verification group;
3. Every member in the verification group will verify the block, sign, and send the signature to each member in the verification group;
4. After verifying each group member, after collecting the signatures of a threshold number of others, the group signature is generated and broadcast to the entire network.
    - Block production speed: 1 block/second;
    - Group Lifecycle: 2 hours;
    - Block distribution cycle: 10 hours (36000 blocks), once every 36,000 blocks;
    - Block rewards: A single block reward is calculated based on the current output mechanism;
    - Block distribution: Single block rewards are distributed according to distribution rules.

g. Becoming a Proposal/Validation Node & Block Rewards

The following content refers to Rangers Mainnet nodes only.

i. Proposal Nodes

It requires staking of 2000 RPG to become qualified of being a proposal node. With Rangers Protocol's development and the governance mechanism's improvement, RPG's number staked as proposal nodes will continue to be adjusted. RPG cannot be unlocked during the period from the stake to block reward distribution. It can only be unlocked after the node reward is issued (10 hours). Each node can stake once in each block distribution cycle. When the rewarded proposal node distributes RPG, it will be done according to each node's RPG stake ratio.

- After the block is generated, the proposal group will receive 24.5% of the total block rewards.
- Each block-generating proposal node will get 7.35% of the total block rewards individually.
- All nodes in the proposal group, including the block-generating one, will share 17.15% of the remaining rewards according to the nodes' stake ratio.

ii. Verification Nodes

It requires a minimum staking of 400 RPG to become qualified as a verification node and later a candidate verification node. Rangers Mainnet sets no restriction on the verification node application; a qualified verification node can enter the random

pool by staking and then waiting to be selected into a verification group. A candidate verification node (for short, candidate node) can be selected into multiple verification groups simultaneously. The maximum number of verification groups that a candidate node can join is calculated by its staking value divided by 400, rounded down. The more a candidate node stakes, the more verification groups it can join simultaneously.

Rangers Mainnet currently selects 5 to 10 members into a verification group. And the genesis group contains 20 members. The verification group members are randomly selected following the VRF consensus mechanism. Therefore, there exists the possibility for a candidate node not being selected into any verification group.

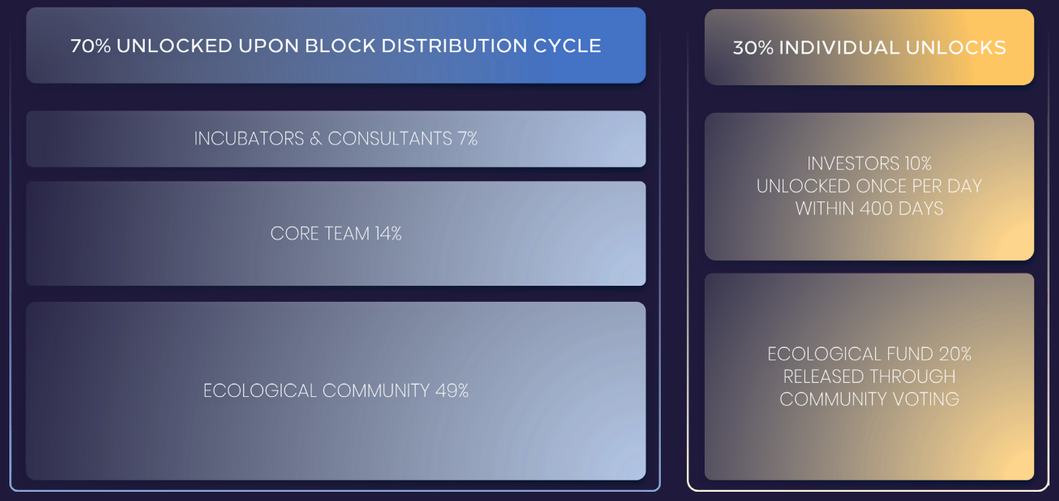
- If the current number of awaiting candidate nodes is below 10, as long as they're in an active-responding status, they would all be selected into the upcoming verification group.
- If the current number of awaiting candidate nodes is above 10, the father group would randomly select 10 out of them.

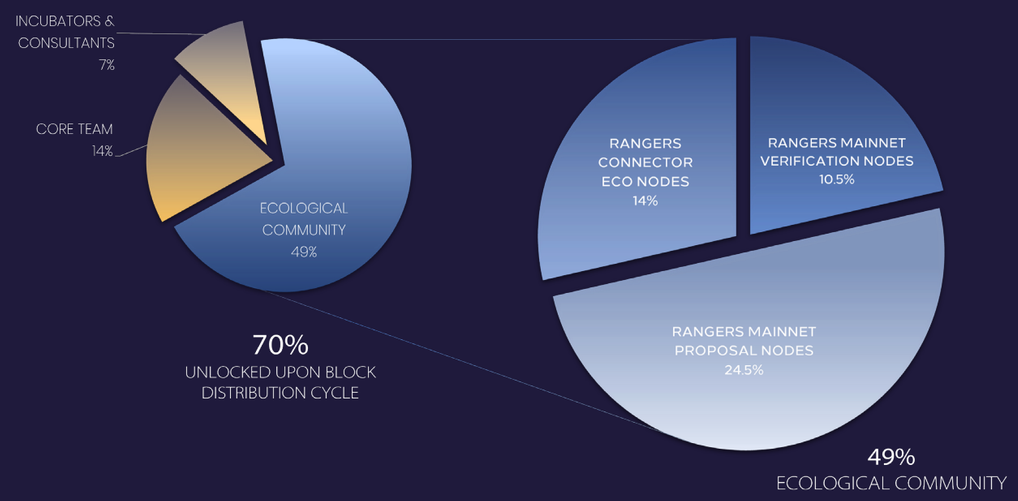
The possibility for each candidate node to be selected into a verification group is the same regardless of the value staked.

The father group starts selecting the next verification group based on a certain block height without having to wait for the latest verification group to be dismissed. The selection for the next verification group will initiate as long as there are plenty of candidate nodes awaiting (a minimum of 5). Candidate nodes that weren't selected into the latest verification group have the opportunity of joining the upcoming one.

A verification node can increase its staking at any time and for unlimited times without having to wait till the current distribution cycle concludes. During the period from staking to block reward distribution, RPG cannot be unlocked. It can only be unlocked after the node rewards are issued (10 hours). The RPG distribution for the rewarded verification node is based on its RPG stake ratio.

- After the block is generated, the verification group will receive 10.5% of the total block reward. All nodes in the verification group will be rewarded according to the nodes' stake ratio.





09. Ecosystem Construction

a. Foundation

Rangers Protocol Foundation is mainly used for ecosystem construction, market promotion, healthy system operation, and community maintenance. Besides, some funds are used for investment to promote ecological development while maintaining the foundation's long-term sustainable operation.

The foundation shall fulfill the following obligations:

1. Organize an open-source community or technology outsourcing team to complete Rangers Protocol's launch and iterative upgrades.
2. Develop the market and build an application ecosystem.
3. Support or invest in Rangers Protocol-based dapp developers.
4. Prevent and punish behaviors unfavorable to the Rangers Protocol ecosystem and maintain the system's healthy growth..

At the same time, the foundation enjoys the following rights:

1. Initiation of voting proposals.
2. Security deposits for forfeiture.

Rangers Protocol Foundation only has the right to initiate a proposal for the entire system's governance. Then the community will vote to decide whether the proposal is finally implemented. In terms of community governance, the foundation can initiate proposals including but not limited to:

1. Modification of system parameters.
2. Proposal improvement and resource pricing usage.
3. Penalties for inaction or evil done by the proposal nodes.
4. Penalties for inaction or evil done by the verification nodes.
5. Punishment for evil done by dapp developers.
6. Other malicious acts

b. Community Ecosystem

As a decentralized, game-focused solution, Rangers Protocol Foundation development is inseparable from the community's support. Rangers Protocol Foundation actively organizes and establishes communities with different functions, including ecological governance, developers, and token holder communities.

Regardless of the community's function, the goal of existence is to promote healthy and stable development.

c. Proposal Nodes

Ecosystem users pay tokens as a guarantee and become a proposal node through community voting. As a proposal node, users must fulfill the following obligations:

1. Stake not less than the specified amount of security deposit.
2. The investment performance is good, and the server with a good network is used as the proposal node.
3. Guarantee long-term online activity.
4. During events, complete the tasks that need to be completed for node roles.

Correspondingly, the rights enjoyed by users include:

- Income issued in the form of tokens

After the user is selected as a proposal node, the server performance and network performance must be guaranteed. Suppose the proposal node cannot be packaged to generate a witness unit within the specified time due to server or network reasons. In that case, it will be treated as a lost block and recorded in the proposal node's statistical information, which will affect the distribution of the node.

d. Verification Nodes

Ecosystem users become candidate verification nodes by staking and are randomly selected as the contract's verification nodes responsible for executing the contract when the contract is created or executed. As a verification node, users need to fulfill the following obligations:

1. Hold a one-time stake on the verification node deposit.
2. Maintain a good network and stay online for a long time.

At the same time, the verification nodes enjoy the following rights:

- Get income issued in the form of tokens

e. Developers

The foundation will regularly hold development or game grants and other activities

to attract developers early. Winning users or teams can directly receive token rewards, and the foundation will further incubate applications into commercial ones.

Developers need to fulfill the following obligations:

1. Pay specific tokens as a deposit and submit application materials to become a certified dapp developer. Only certified dapp developer applications will appear in the Rangers Protocol ecosystem application.
2. Smart contracts must not commit malicious acts; otherwise, they will be punished.
3. Pay a specific token to deploy the application.

10. Governance Mechanism

The following content refers to Rangers Mainnet nodes only.

a. Roles Involved in Governance

1. Governance Nodes

- Proposal Nodes

Proposal nodes are generated using the algorithm mechanism of VRF+BLS. The user or organization uses Rangers Mainnet to apply to the foundation for the proposal node election. After paying the deposit, they can participate in the election of the proposal node. The first batch of proposal nodes is generated through the foundation's directional invitation to the co-builders of the ecology. After the first round of the election, the expansion and re-election of proposal nodes will be carried out through community voting.

- Verification Nodes

The token holder can freely join the Rangers Mainnet verification network and become a verification node after running a node and pledging a certain amount of tokens.

Both proposal nodes and verification nodes can be the candidates for governance nodes. Other users can entrust their tokens to the governance node candidates. The system will rank the candidates according to their total equity (staking + delegation). The top 200 candidates will be elected as governance nodes.

2. Currency Holders: all RPG token holders
3. Core Developers: core developers jointly building the Rangers Protocol infrastructure and community.

b. Distribution of Rights

i. Governance Nodes

- Initiate a proposal
- Vote on the referendum proposal
- Vote on the non-referendum proposal
- Second the proposal

ii. Token Holders

- Initiate a proposal
- Vote on the referendum proposal
- Second the proposal

iii. Core Developers

- GitHub code control
- Proposal Review
- Proposal implementation

C. Proposal Classification

The decision-making right should rest with the “stakeholders,” which means the right belongs to the people. However, the implementation of the referendum needs to consider issues such as implementation costs, turnout rate, professionalism, and governance efficiency. This should not be the normal state of governance but the way of governance in the event of major differences. Therefore, Rangers Protocol’s governance adopts a combination of indirect democracy and direct democracy. Its core principle is: under normal conditions, governance nodes vote for governance, which is indirect democracy, while under major differences, the community is governed by public voting, which is direct democracy.

i. Governance Nodes

The referendum proposal occurs in a rather controversial scenario. Any currency holder can initiate a referendum proposal. The scenarios that require a referendum to produce results are as follows:

- Amend basic rules
- Make a major fork
- Terminate the running chain

For Example:

Proposal Topic	Level of Importance
Revise the verification group scope	Medium
Add new proposal node	Medium
Block height	High
Lowest stake value	High
Reward-distribution ratio for block generation	High
Transaction fee	Medium

ii. Non-referendum proposal

Non-referendum proposals are ordinary proposals, which are initiated by governance nodes and voted to produce results. Non-referendum proposals can be divided into the following types:

- Text proposals: for decisions that need not be implemented
- Software upgrade proposal: to initiate an upgrade vote on the chain to achieve a smooth upgrade
- Parameter modification proposal: to modify manageable parameters such as system parameters
- Account proposal: to freeze or unfreeze accounts (including contracts)
- Incentive proposal: to allocate the balance in the governance fund account
- Cancellation Proposal: to cancel the software upgrade proposal being voted on the blockchain

For Example:

Proposal Type	Proposal Topic	Level of Importance
Parameter Revision	Revise the verification group lifecycle	Low
Parameter Revision	Revise the verification group generation cycle	Low
Parameter Revision	The number of candidate blocks for each block cycle	Medium

Parameter Revision	Bn256, secpk256 curve parameter	Medium
Parameter Revision	The distribution time for block reward	High
Parameter Revision	The effective time for stake unlock	Medium
Parameter Revision	Add new service command to the virtual machine	Medium
Parameter Revision	The max gas amount / contract creation	Medium
Parameter Revision	The max gas amount /contract transfer	Medium
Parameter Revision	The max storage for contract codes	Medium
Parameter Revision	Revise the gas fee of commands, e.g. Store	High
Parameter Revision	Soft fork inspection cycle	Low
Parameter Revision	System upgrade	Low

d. Governance Process

i. Initiate Proposal

Currency holders can initiate referendum proposals, while governance nodes initiate non-referendum proposals. Each proposal should have a corresponding text description stored in the PIP repository on GitHub and managed by the core developer, similar to EIP. To prevent spam proposals, a proposal fee is required for every initiated proposal as its cost.

ii. Screen Proposal

- Referendum proposal: Since the referendum proposal is not the norm, multiple referendum proposals can be initiated on the chain simultaneously. These proposals will be sorted according to the highest margin. The proposal with the highest margin will be selected each month to enter the voting stage.

- Non-referendum proposal: The successfully initiated proposal will directly enter the voting stage. Multiple proposals can be voted on at the same time.

iii. Vote for Proposal

- Referendum proposal:

The core of referendum proposal voting is equity voting, which lasts for two weeks. There are three voting options: support, object, and abstain. Only the tokens that are staked and delegated can vote. The voting adopts the “government node proxy voting + personal voting “ model. The voting weight of the governance node is the sum of its own staked tokens and the number of entrusted tokens. If the delegator and the governance node hold different opinions, the delegator can vote on its own, and its voting weight is the number of delegates, and the voting options corresponding to this weight will be overwritten. During all voting processes, the tokens participating in the voting will be locked until the end of the voting. To alleviate the voting centralization problem caused by the majority of tokens being controlled by a small number of nodes, the number of governance nodes participating in voting should be large enough. If most governance nodes do not agree or do not participate in voting, the proposal will still not pass.

- Non-referendum proposal:

The core of non-referendum proposal voting is governance node voting. As long as the node is elected as the governance node within the proposal’s voting period, it can vote. The voting generally lasts two weeks. The proposal initiator can determine the voting period of the software upgrade proposal according to the situation. The voting adopts the one-governance-node-one-vote system. After the voting starts, the governance node’s own staked tokens will be locked until the voting ends. Except for the software upgrade proposal, there are three voting options for other types of proposal voting, namely: “Yes,” “No,” and “Abstain.”

There is no explicit option for the software upgrade proposal to simplify the voting process. Each governance node can indicate its voting position by upgrading its local node or not. For details, please refer to the upgrading mechanism.

iv. Voting Results Calculation

- Referendum proposal: There are three dimensions for calculating the results of referendum proposals

1. Governance node support rate: the ratio of the number of governance nodes voting for support to the total number of governance nodes eligible to vote;
2. Token support rate: the ratio of the number of tokens voting for support to the total number of tokens participating in the vote;
3. Token participation rate: The ratio of the total number of tokens participating in the voting to the total number of staked tokens.

When all: Governance node support rate> P%, Token support rate> Q%, and Token participation rate> K%, the proposal is approved. Otherwise, the proposal is not approved.

- Non-referendum proposal: There are two dimensions for calculating the results of referendum proposals

1. Governance node support rate: the ratio of the number of governance nodes

voting for support to the total number of governance nodes eligible to vote;

2. Governance node participation rate: the ratio of the number of voting governance nodes to the total number of governance nodes eligible to vote;

When both: Governance node support rate > M% and governance node participation rate> N%, the proposal is approved. Otherwise, the proposal is not approved.

The support and participation rates corresponding to different types of proposals are as follows:

Type	Support Rate	Participation Rate
Text Proposal	> 50%	>= 66.7%
Cancellation Proposal	> 50%	>= 66.7%
Parameter Proposal	> 50%	>= 66.7%
Upgrade Proposal	= 100%	>= 66.7%

e. Upgrade Mechanism

The upgrade mechanism guarantees that the network can continue to iterate and improve. For the different situations that may occur during the operation of the blockchain system, Rangers Protocol will provide targeted upgrade methods, mainly the following four kinds:

- Optimizing upgrade: This type of upgrade is a functional optimization of the current chain version. Each node can decide to upgrade or not according to its actual situation without affecting the consensus.

- Voting upgrade: This type of upgrade happens for adding new features or when the consensus mechanism is affected by patch repairing. This upgrade requires a software upgrade proposal to be initiated on the chain, and the voting results will determine whether to implement the upgrade or not. If the proposal passes, the node needs to complete a smooth upgrade without interruption of the network. The focus will be explained later.

- Repairing upgrade: When a node cannot participate in the consensus as usual due to a low version or an abnormal transaction, the governance node can resume participating in the network consensus by installing a new version of the software.

- Snapshot upgrade: When the blockchain system encounters a major abnormality that causes the entire chain to fail to produce blocks, as usual, a snapshot can be generated based on the previous normal network state. The network can then be restored based on the snapshot.

f. On-Chain Voting Upgrade Mechanism

i. Initiate Upgrade Proposal

Only governance nodes can initiate upgrade proposals, and a proposal fee higher than regular transactions needs to be paid when initiating. The following parameters need to be provided in the software upgrade proposal parameters:

- The version number of the upgrade target.

- The ID of the file the upgrade information of which GitHub describes, PIP-ID, must be unique.

- The number of consensus rounds for voting on the upgrade proposal is N. This parameter will be used to calculate the voting cutoff block height, the designated voting cutoff block height for the Nth consensus round at the beginning of the current consensus round.

There can only be one software upgrade proposal in process on the chain. When there is already a software upgrade proposal or parameter proposal in voting on the chain, other software upgrade proposals cannot be initiated. In case of special reasons or emergencies, when it is necessary to initiate a new software upgrade proposal immediately, a cancellation proposal needs to be initiated to cancel the ongoing software upgrade proposal.

Cancellation proposal description: A cancellation proposal can be initiated only when an upgrade proposal is voted on the chain. The following parameters are required to cancel a proposed transaction:

- To-be-canceled upgrade proposal transaction hash

- The ID of the file that GitHub describes the upgrade information, PIP-ID, must be unique.

- The number of consensus rounds for voting on the cancellation proposal. The voting cutoff block height calculated by this parameter cannot exceed the voting cutoff block height of the canceled upgrade proposal.

ii. Proposal Voting Upgrade

After the software upgrade proposal is successfully initiated, it enters the voting stage. Only governance nodes can participate in voting. That is, node stake accounts can only initiate voting transactions. Before voting, local nodes need to be upgraded, and votes are counted on a one-node-one-vote basis.

The voting options of support, object, and abstain are not set in the voting transaction of the software upgrade proposal. Instead, they express their position through node behavior, as follows:

- Supporters: After updating the local node version to the version in the proposal upgrade, vote on the upgrade proposal;

- Neutral: You can choose to upgrade the node, but do not vote, and initiate a version declaration transaction to declare that the node has been upgraded so that you can participate in the consensus as usual regardless of whether the proposal is passed or not;
- Opponents: There is no need to upgrade the local node or vote.

The following parameters need to be provided to upgrade proposal voting transactions:

- Hash for initiating the proposal transaction;
- The actual version number of the node. This version number needs to be the same as the version number of the upgrade destination in the voting to vote successfully;
- Node signature. The signature is the signature of the node's private key to the version number of the node.
- Although the node has been upgraded during the voting period, the logic currently running is still the logic of the old version. Switch to the new version of the logic after the implementation is complete.

iii. Statistics of Voting Results for Upgrade Proposals

At the end of the voting block, the voting results on the upgrade proposal are counted. If the support rate of the proposal reaches 66.7%, the proposal is voted through and enters the implementation stage.

iv. Proposal Implementation Upgrade

At the end of the voting block, the voting results on the upgrade proposal are counted. If the support rate of the proposal reaches 66.7%, the proposal is voted through and enters the implementation stage.

Due to the randomness of the governance nodes selected by VRF and to not affect the consensus, when we implement the upgrade, we need to ensure that the verification nodes in a particular consensus round are all upgraded nodes.

Therefore, when the voting deadline for the proposal is high, the support rate of the proposal reaches 66.7%. The upgrade will be implemented in the first block of the following consensus round, and nodes that have not been upgraded will no longer be selected to participate in the consensus. In the current settlement cycle, the eliminated unupgraded nodes will not be selected by the VRF to participate in the consensus. However, they still enjoy the stake income of the current settlement cycle.

v. Version Statement

Since there may be data incompatibility between different versions, the node version on the chain should be controlled to avoid consensus failure due to version issues.

Therefore, Rangers Protocol has introduced a version statement. By initiating a version statement, the node indicates that its node version is consistent with the current chain version or the target version number in the software upgrade proposal voting. In such a way, it can participate in the consensus before and after the upgrade.

When the node and chain versions are inconsistent (the first two digits of the version numbers are different), the node will not be selected to participate in the consensus, even if its stake is high. At this point, the node can declare that its node is consistent with the chain version by initiating a version declaration transaction to participate in the consensus in the subsequent settlement cycle as usual. A version statement consistent with the upgraded version can be initiated when there is a voting software upgrade proposal on the chain. The version statement does not represent a vote. After the upgrade proposal is voted through, it is stated that the nodes with the same version number as the upgrade destination can participate in the consensus as usual even if they have not voted.

vi. Quick Upgrade

Initiating an upgrade vote on the chain is a serious matter. In theory, there should be no possibility of revoking the proposal. All results should be left to the governance node for voting. But ours only allows one voting software upgrade proposal on the chain, so when an emergency needs to be quickly upgraded, if there is an unprocessed proposal on the chain, it will directly affect the processing speed of the emergency. Therefore, we introduce the cancellation proposal initiated by the governance node, and the voting cycle can be determined by itself. However, it must be within the voting cycle of the canceled proposal. By initiating a cancellation proposal and quick response of each node, the software upgrade proposal that is being voted on can be canceled in a short time so that the emergency plan can be quickly implemented. Only when there is a voting upgrade proposal on the chain, a cancellation proposal can be initiated. Once a cancellation proposal is commenced, it must be implemented, so we advocate using cancellation proposals only in emergencies.

The transaction to cancel the proposal requires the following parameters:

- The canceled upgrade proposal transaction;
- The ID of the file describing the upgrade information on GitHub, that is, PIP-ID, must be unique;
- The number of consensus rounds for canceling a proposal to vote. (The voting block height calculated by this parameter cannot exceed the voting block height of the canceled upgrade proposal)

g. Governance Parameters

Governance nodes can modify some system parameters by initiating parameter governance proposals. In order to avoid problems caused by the cross-implementation of parameter proposals and upgrade proposals, when there are voting upgrade proposals or parameter proposals on the chain, it is not allowed to initiate new parameter modification proposals. The voting period for a parameter proposal is two weeks.

h. Reward and Punishment Mechanism

The purpose of designing a punishment mechanism is to ensure that nodes and users are honest and trustworthy. Inaction or malicious behavior will be punished. Unlike the direct penalty mechanism of agreements such as Plasma, Rangers Protocol uses incentives in the economic model to encourage nodes to be honest and trustworthy.

1. Reward

- Proposal rewards: Proposal rewards are automatically issued to the proposal initiating account after the proposal has been voted through.
- Voting rewards: After the voting starts, the tokens participating in the proposal voting need to be locked until the voting ends. Therefore, voting rewards are proportional to the length of the voting lock-up time, and will be distributed to each voting account at the end of the proposal voting.
- Developer rewards: A proposal needs to be initiated on the chain, the voting results of which will determine whether to issue the rewards or not.
- Loophole bounty: After confirming the existence of the loophole, a proposal needs to be initiated on the chain, whose voting results will determine whether to issue the bounty or not.

2. Punishment

The purpose of designing a punishment mechanism is to ensure that nodes and users are honest and trustworthy. Inaction or malicious behavior will be punished. Different from the direct penalty mechanism of agreements such as Plasma, Rangers Protocol uses incentives in the economic model to encourage nodes to be honest and trustworthy.

Suppose a user does not act for a long time or initiates a malicious attack while serving as a proposal node or verification node. In that case, the foundation can trigger the contract to freeze the user's stake, cancel the user's application for the role of the proposal/verification node, publicize it to the community, hold votings, and then forfeit a certain degree of fines towards the staked tokens. Similarly, certified developers must ensure the absence of malicious behavior in their developed applications or products. If they are found to be so, the foundation can also initiate penalties and confiscate developers' staked tokens. The confiscated staked tokens are transferred to the foundation to help the further construction of the community.

- Proposal nodes

In the financial model, we mentioned that the proposal node alone receives 7.35% of the total block reward. So if the proposal node does not act or do evil, it will lose this part of the reward, unwise for proposal nodes.

- Verification nodes

Assuming that the verification node does not act and the group verification fails, the proposal node will select another verification group. This will result in no benefit for all nodes in this group.

- Governance nodes

If a dishonest node achieves the upgrade by disguising its version, when the chain is successfully upgraded, and the governance node is selected to participate in the consensus, the block generation rate will be low because the consensus cannot recognize the generated block. The node will thus be punished by the system and even directly disqualified as a verification node.

i. Governance Fund

The governance fund comes from the foundation. Each year, a fixed proportion of funds is allocated from the foundation's account to the governance account. The balance of the governance account is allocated for incentives and salary distribution through proposal voting. When the proposal is voted through, it will be automatically issued through multi-signature.

11. Summary of Token Design, Ecosystem Construction, &Governance Mechanism

The token economy design itself is a virtuous economic cycle, enabling long-term currency holders to lock their positions and gain benefits. All users in the system will have corresponding benefits. Developers who hold tokens can obtain appropriate dapps development resources without worrying about user acquisition and infrastructure performance limitations and constraints. Users can also focus on the new experience of dapps and digital assets. And system maintainers also get their due rewards.

Besides, Rangers Protocol's reasonable token design is based on a complete distribution mechanism, incentive income, and VRF's truly random algorithm. RPG's consumption, circular use, and inherent value provide a powerful growth engine for itself. It will be a qualitative leap to the underlying protocols of the existing blockchain industry.

12. The Project
Team, Partners & Investors

a. Team

ZKSUN

CEO/Founder. Technical expert in Shanda Group Innovation Institute, engaged in the construction of your Instant Message software system. Firmly believes that the blockchain system is the next-generation network form and the infrastructure of the 5G and 6G era. Proficient in the research and development of distributed systems, proficient in the architecture of large concurrent systems, and has long been engaged in the research and development of large-scale Internet infrastructure. Participated in the Rangers Protocol's framework creation.

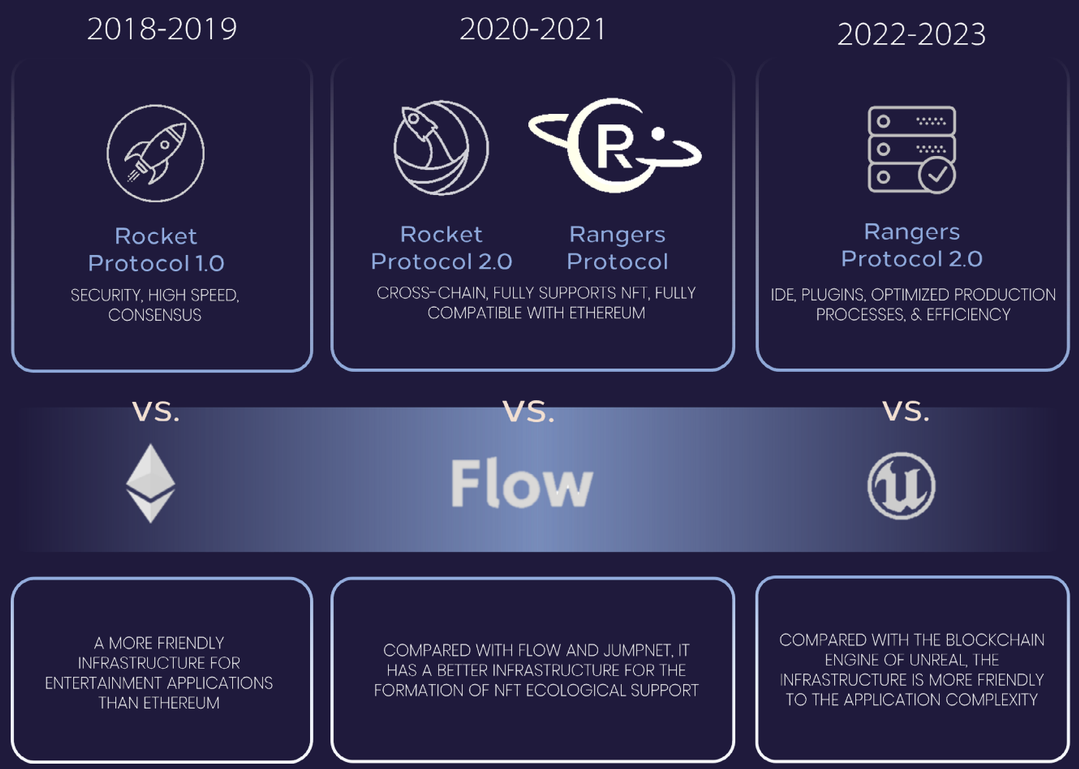
b. Partners

c. Investors

13. The Project
Roadmap

a. Positioning and Goals

Rangers Protocol's core positioning is to be a Web3 engine infrastructure. Rangers Protocol's long-term goal is to build a Web3 Engine that is friendly to decentralized application developers and users. Rangers Protocol's short-term goal is to become a secure, high-speed, cross-chain decentralized application blockchain infrastructure supporting NFTs and digital assets compatible with Ethereum (or adopting a consistent architecture with Ethereum).



b. Rangers Protocol Roadmap Overview

Since founded in 2018, Rangers Protocol has achieved impressive milestones in its technology breakthroughs, business fundraising, and market development.

- Through dedicated innovations from its core teams, Rangers Protocol has built and delivered consistent upgrades for popular blockchain infrastructure including Rangers Mainnet, Rangers Connector, and Rangers REVM; The team is currently developing Rangers Sub-Chains as well.
- With an experienced board of advisors, Rangers Protocol has completed successful fundraisings, backed by high-quality investors, and cooperated with industry-leading projects.
- Always keeping developers and user communities at its heart, Rangers Protocol has reached global influence in the Web2 and Web3 world. Upcoming grants would further enhance Rangers Protocol's community co-creation vision.

This section only showcases some highlights of the Rangers Protocol roadmap. For more detailed information regarding Rangers Protocol's technology, business, and marketing success, please visit the Rangers Protocol official website.

2021

	Q1	Q2	Q3	Q4
BUSINESS	Received $1.2M in seed round financing	Received $3.7M in institutional fundraising Reached partnership with Parsiq	Deployed BlueStone, the first DeFi protocol	$420k IDO on Polkastarter Released $RPG on PancakeSwap & Uniswap Partnership with Polkastarter, UniArts, Litentry & NFTMart
TECH Rangers Mainnet	Ethereum NFT compatibility	Ethereum NFT compatibility	Launched the first Testnet	EVM enhancement Launched Robin testnet Launched Rangers mainnet
TECH Rangers Connector	Multi-signature mechanism	Upgraded to the PoW consensus mechanism	Cross-chain solution based on distributed signature Upgraded to VRF+TSS (ECDSA) consensus mechanism	Developed a Secure Multi-Party Computation Chain based on VRF+TSS (ECDSA)

2022

	Q1	Q2	Q3	Q4
BUSINESS	Reached partnership with a third-party light wallet	Deployed DeHero, the first gaming dApp	Launch RPG on CEX Reach partnerships with more middlewares Build a comprehensive ecosystem	Integrate more dApps Build the developer community
TECH Rangers Mainnet	Integrated a mass-oriented light wallet Developed node toolsets	Launched the sub-chain plan Deployed the node toolset *	Develop sub-chain Maintain infrastructure stability	Enhance sub-chain Keep tech upgrades and the Mainnet stability
TECH Rangers Connector	Developed a Secure MPC Chain based on VRF+TSS (ECDSA)	Governance of the MPC Chain	Upgrade to a Secure MPC Chain based on VRF+TSS (ECDSA)	Become compatible with more public chains besides ETH and BNB Chain

* Check our existing and upcoming tools here

Our Media

linktree

https://linktr.ee/rangersprotocol