RANGERS

PROTOCOL

Rangers Protocol White Paper

V. 1.1

Oct. 2021

VIRTUAL WORLDS BLOCKCHAIN INFRASTRUCTURE

https://linktr.ee/rangersprotocol

White Paper
Table of Content

01. White Paper
Introduction

01.1 Preface

Rangers Protocol is a future-oriented virtual world blockchain infrastructure incubated by MixMarvel, integrating cross-chain, NFT, EVM, and distributed network protocols and professionally supports NFT and complex applications. As a high-performance chain group that can realize the EVM multi-chain contract interoperability, Rangers Protocol serves all entrepreneurs who want to explore the blockchain world. It allows pioneer developers to freely try out diverse content and applications in the Rangers Protocol ecosystem without permission.

For this purpose, Rangers Protocol has gathered a group of senior technical engineers. It took three years to develop an underlying technical solution with a clear framework and functions. This infrastructure can provide developers and users with the simplest operation, high performance, and high applicability.

From the technical point of view, Rangers Protocol is divided into two parts: Rangers Engine and Rangers Connector.

Rangers Engine is the core part 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 responsible for completing the interconnection with various public chains, and its primary function is to provide cross-chain services for developers and users. It includes:

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

This white paper comprehensively describes the design philosophy, methodology, and core technology of Rangers Protocol, and finally falls into the specific implementation, and uses simple and readable language to convey information as much as possible. Rangers Protocol strives to enable users who read this white paper to master the essentials of Rangers Protocol in no time. In addition to the current piece, our team will provide independent yellow papers, developer documents, and other documents to elaborate on using Rangers Protocol.

01.2 Dictionary

Before reading this article, 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: Also called 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 article 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, coAmpatibility, 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 Ethereum-compatible, widespread 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 a decentralized application platform. By providing an infrastructure with a built-in Turing complete programming language, anyone can create 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. Rangers Protocol is committed to providing a blockchain infrastructure for the virtual world. 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-out to be a high-performance chain group. In short, with Rangers Protocol, we solve 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 v-world standard protocol.

02. About Rangers Protocol

Rangers Protocol is a future virtual-world-proofing blockchain infrastructure fully compatible with Ethereum and natively supports NFT and complex applications.

We integrate cross-chain, NFT, and EVM protocols and expand on this basis, allowing developers to freely create complex decentralized applications that adapt to various scenarios while giving users an experience similar to Internet applications.

Consensus

It integrates an efficient VRF+BLS consensus mechanism to solve the problem of high-frequency trading. Rangers Protocol produces a block every second. Compared with the traditional PoW block/minute generation, the efficiency is improved by a hundred times. It minimizes the possibility of network congestion and reduces usage costs.

Real-Time Transactions

It integrates real-time confirmation of transactions to solve interactive problems. Rangers Protocol can return the real-time execution result for most transactions without the user having to wait for the block to be generated. For developers, it is an easy-to-use synchronization mechanism with instant response.

Bridge

It solves the asset migration problem through Distributed Signature technology. Rangers Protocol adopts a Secure Multi-Party Computaion blockchain technology that is based on VRF+TSS consensus mechanism, combined with a distributed signature verification smart contract deployed on public chains, to ensure the security of users' asset cross-chain process.

NFT Protocols

It incorporates protocols such as ERC-721 to standardize NFT as a standard for digital assets. Rangers Protocol further extends its features, including life cycle management, a new data structure supporting data reuse, and data rights management based on Dapp latitude, on top of the ERC-721.

We have integrated an efficient VRF+BLS consensus mechanism to solve the problem of high-frequency trading. Rangers Protocol 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.

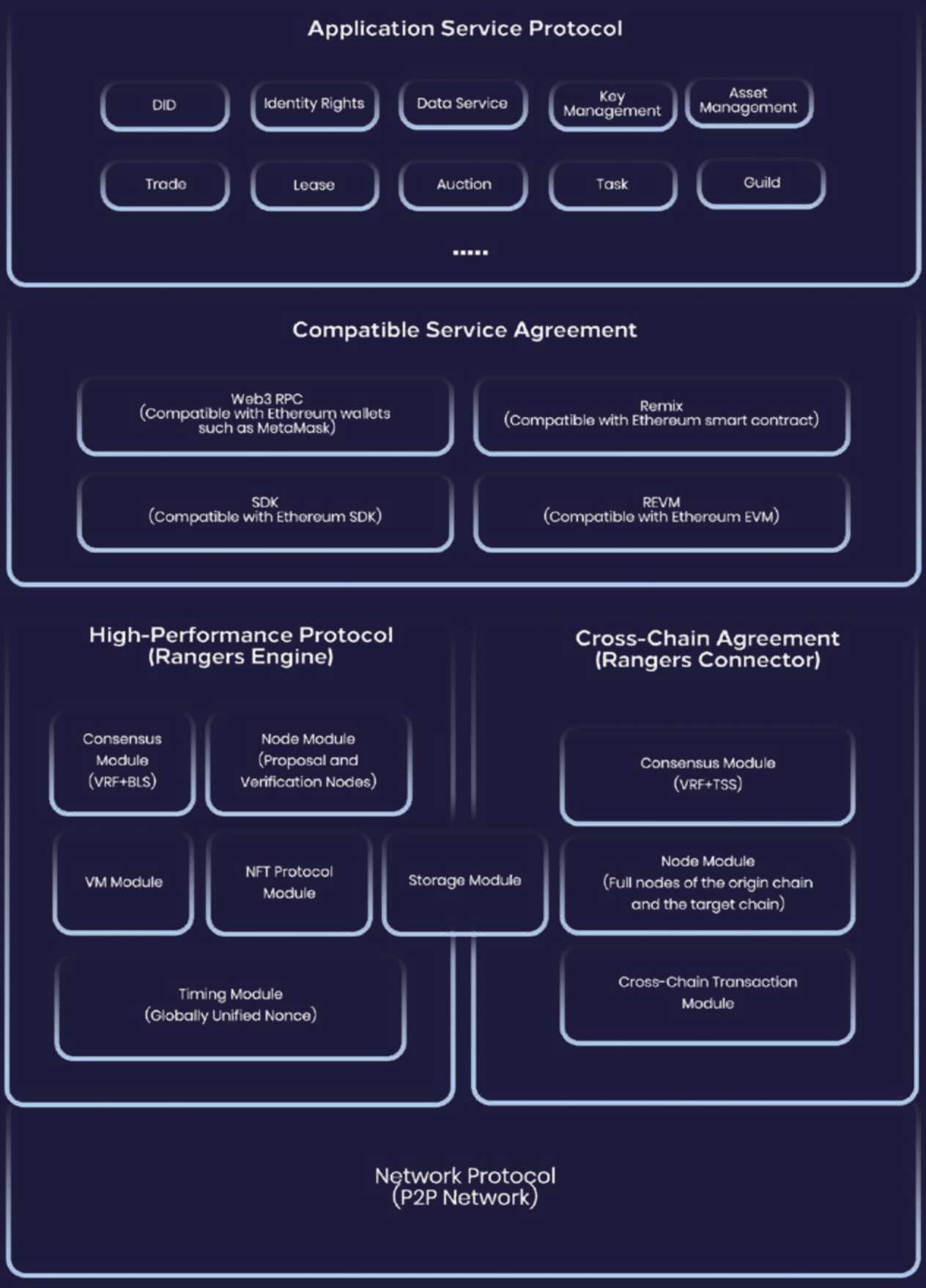
We have also integrated a cross-chain solution based on distributed signatures to solve asset migration problems. One of Rangers Protocol's visions is to become the bridge for blockchain assets' circulation and connect various public chains. As a result, digital assets will run smoothly between Rangers 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 public chains – Rangers Protocol 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, we 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 need to call back/poll/subscribe to messages to process business logic, contrary to mainstream developers' habits. 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.

We have incorporated protocols such as ERC-721 to standardize the data structure of digital asset NFTs. On its basis, Rangers Protocol has expanded its features, including life cycle management, a new data structure that supports data reuse, and data rights management based on decentralized applications.

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:

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

2. 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).

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

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

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

04. Technical Features

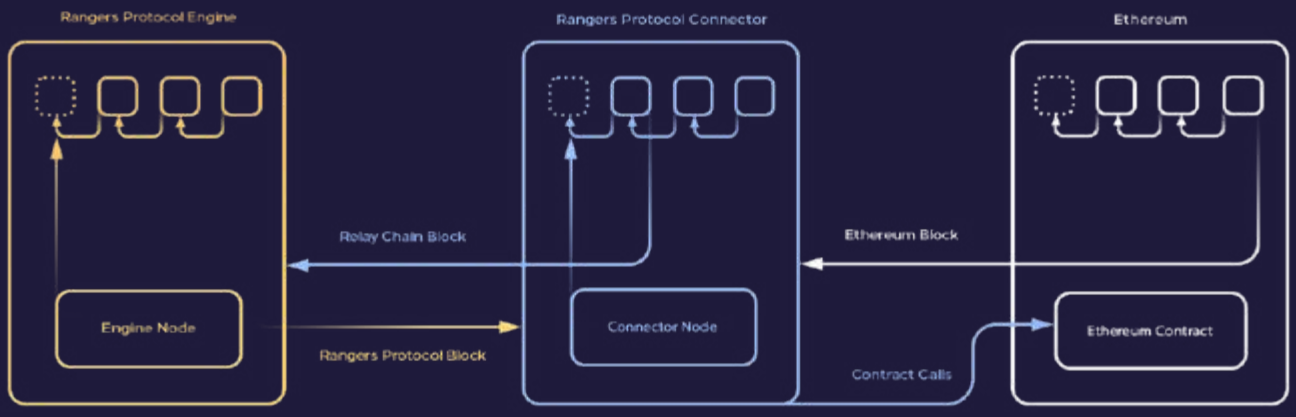
04.1 Composability and Interoperability

Bridging and Cross-Chain Technology

One of Rangers Protocol'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 public chains – Rangers Protocol 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.

The cross-chain architecture of Rangers Protocol is shown in the following scheme. Rangers Protocol Connector node is the primary generating node of the relay chain. In contrast, Rangers Protocol Engine node and Ethereum are the actual bearers of cross-chain data.



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

1. **Public chain assets to Rangers Protocol**

- Locked transactions that involve users sending NFT assets lock the Ethereum NFT assets to a specific contract;
- The Ethereum public chain packs these transactions into blocks;
- Rangers Connector node receives the public chain block through the P2P network and parses 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 blocks according to the relay chain's PoW consensus and pack cross-chain transactions when the blocks are created;

- Rangers Engine nodes receive the relay chain blocks and verify them according to the relay chain's PoW 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 the public chain

- The user submits an application transaction to Rangers Engine for the NFT to be listed on Ethereum. The transaction contains the NFT to be added to the blockchain and the corresponding blockchain address;
- After the Rangers Engine node verifies the user's NFT assets, it will be locked. At the same time, package the transaction into blocks;
- Rangers Connector node receives the block information from Rangers Engine. 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 blocks according to the relay chain's PoW consensus and pack cross-chain transactions when the blocks are created;
- 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.

NFT Standard 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 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.

04.2 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. Generally speaking, the function'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 Protocol, 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. In contrast, verification nodes are randomly divided into groups 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 Protocol uses the combination of BLS and VRF to allow nodes to cooperate and improve the truly random number system's stability and security.

04.3 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.

04.4 Compatibility: Compatible With Ethereum Virtual Machine

Rangers Protocol is a smart contract chain 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, deployed to Rangers Protocol.

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 we already complete through Rangers Protocol's cross-chain solution.

Ethereum's code compatibility job includes the following aspects:

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.

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.

EVM

EVM is a state transition engine on Ethereum responsible for the deployment and invocation

of smart contracts. Rangers Protocol has a complete EVM implementation, 100% compatible with the EVM on Ethereum. From the perspective of functional characteristics, account, and even the key used to sign the transaction, Rangers Protocol compatibility with the existing Ethereum is consistent.

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.

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.

04.5 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

05.1 System Introduction

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 user;
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.

Rangers Engine

Rangers Engine 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.

Rangers Connector

Rangers Connector is responsible for completing the interconnection with other public chains. Rangers Protocol 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 relay chain 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 Protocol Connector.

- **Full Rangers Protocol Client**

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

1. Connects to Rangers Protocol mainnet to obtain Rangers Protocol blocks through P2P;
2. Verifies the legitimacy of the block header based on VRF+BLS (Rangers Protocol Consensus Algorithm);
3. Executes the transactions packaged in the block, updates the data status of the local Rangers Protocol 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 Protocol chain while maintaining the local canonical chain, including fork processing;
6. Packs cross-chain transactions into the local Rangers Protocol 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 Protocol Connector transaction pool.

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

05.2 Consensus Mechanism

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 Protocol, 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 Protocol is mainly used to aggregate each member's signature in the verification group for the candidate block to generate the verification group signature.

Verification and Proposal Nodes

Rangers Protocol 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.

05.3 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.

05.4 Information Upload Process

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 node 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 blocks 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.

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 member. 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, 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.

05.5 Access Process

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 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.

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 contract 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, which has supported 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

06.1 Rocket Protocol 1.0

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

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

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).

06.2 Rocket Protocol 1.5

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.

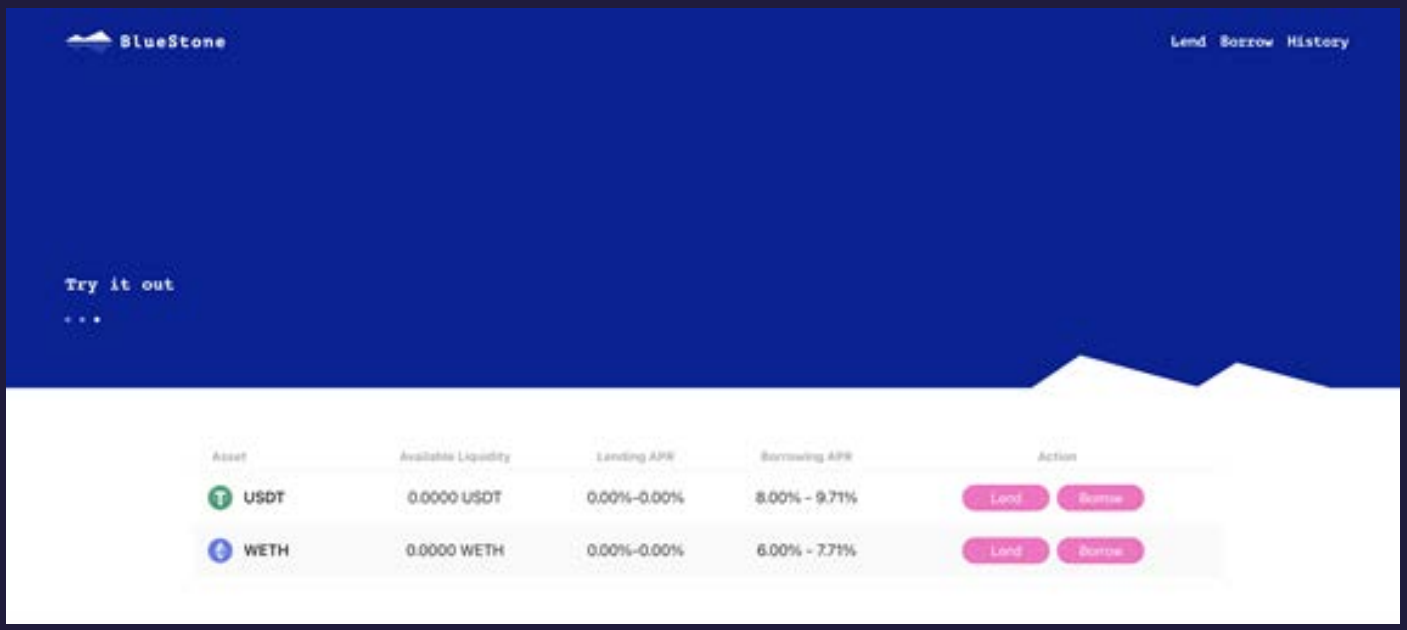
After the launch of Rocket Protocol 1.5, the HyperDragons application was released on ETH, Tron, ONT, and Ant Blockchain almost simultaneously. The Ant Blockchain-based HyperSnakes appeared in the popular section on the Alipay homepage during March 2020. It withstood the extreme test of adding 20,000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

06.3 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 businesses. 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.

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: 9527).

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.

07. RPG Token Design

07.1 Token Definition

RPG (Rangers Protocol Gas) is the Rangers Protocol ecosystem token, with a total supply of 21 million pieces.

RPG is the native token of Rangers Protocol. There are also RPG tokens issued on ERC20 and BEP20 format.

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 registered users to participate in the system's operation.

07.2 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. General network-compatible devices, rather than customized professional devices, can become nodes. In terms of security, VRF truly random numbers select groups to ensure that the working group is unique at a certain altitude. The periodic Check Point mechanism ensures that the block data is "final." It eliminates problems such as long-range attacks and private mining.

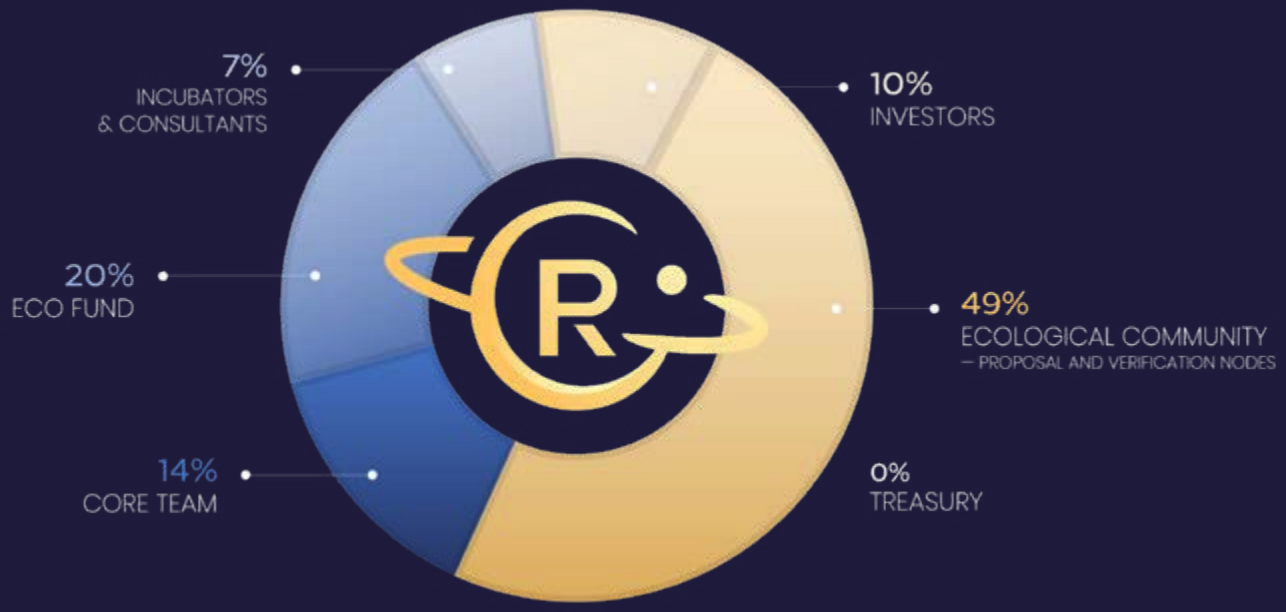
In terms of design, the token economy system must create real value for each user and encourage users to increase their productivity. Therefore, Rangers Protocol designed the Protocol Principle and Transparency Principle. Protocol Principle: an excellent economic system relies on protocol behavior and 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.

07.3 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 applications deployed on 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.

07.4 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 is divided into the proposal and ecological nodes**

- Proposal nodes (35%): join through RPG-staking election and provide special hardware
- Verification nodes (14%): stake RPG, and provide required hardware

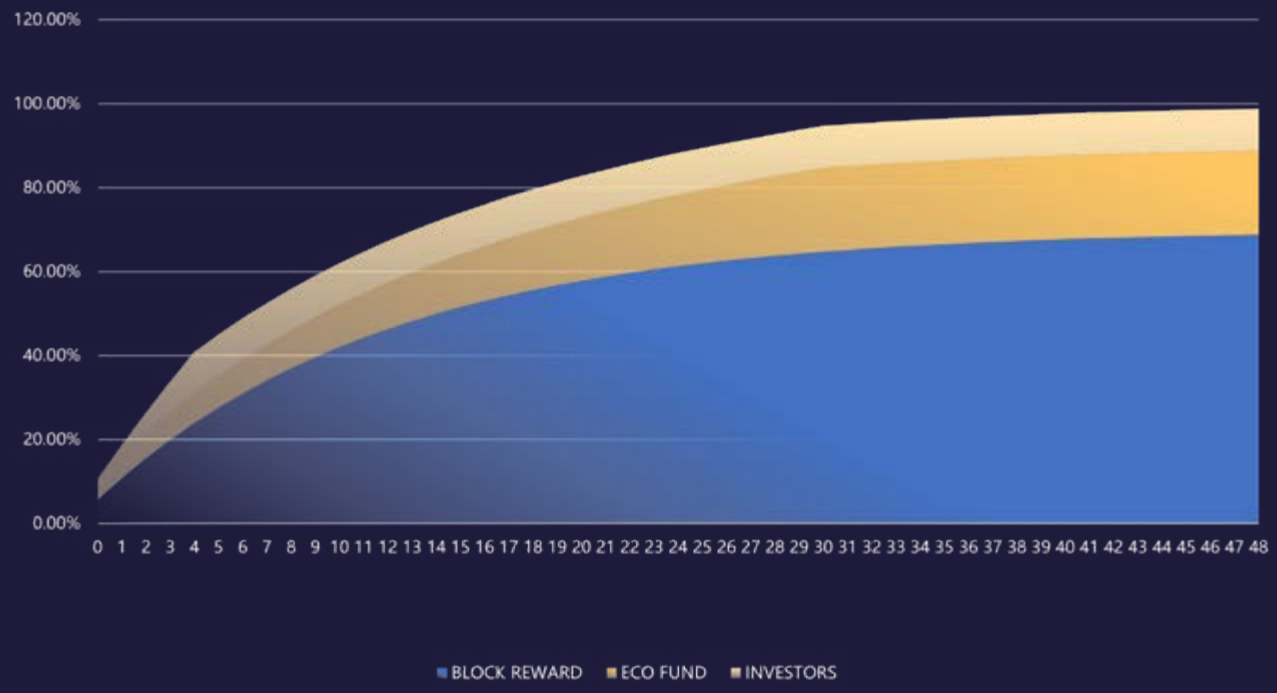
5. **Ecological fund (20%): The unused amount is locked, community voting will be held, and relevant announcements made on the foundation website upon use**

- 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

07.5 Supply Model



07.6 Block Production Process and Incentive Mechanism

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 broadcasted.

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 algorithm, 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 produced 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.

Within Block Production Process

1. The proposal node is selected from the proposal group based on VRF 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

07.7 Becoming a Proposal/Validation Node & Block Rewards

Proposal Nodes

It requires staking of 1250 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 distributing RPG to the rewarded proposal nodes, it will be done according to each node's RPG stake ratio.

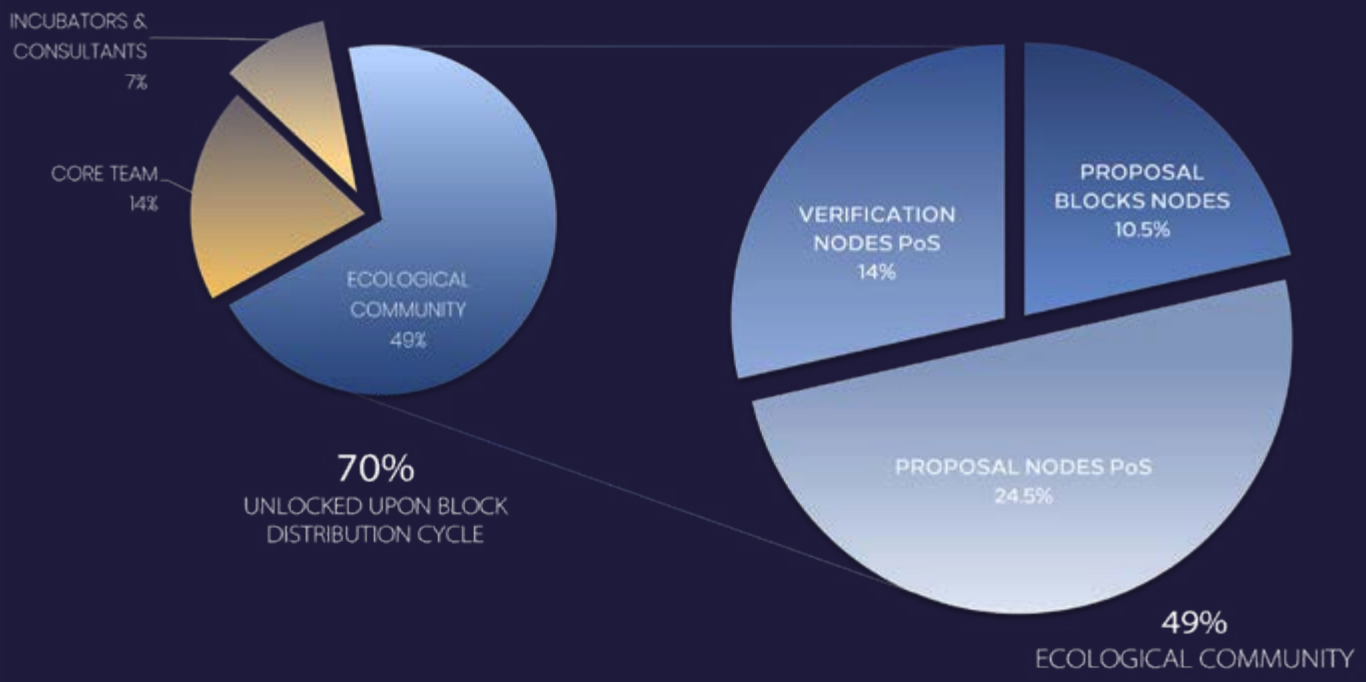
- After the block is generated, the proposal group will receive 35% of the total block rewards.
- Each block-producing proposal node will get 10.5% of the total block rewards individually.
- All nodes in the proposal group, including the block-producing ones, will share 24.5% of the remaining rewards according to the nodes' stake ratio.

Verification Nodes

Any registered user must stake 250 RPG to be qualified to be a verification node. There is no restriction on node application, as long as the stake can enter the random pool, waiting to be selected as a verification node. During the period from the stake to block reward distribution, RPG cannot be unlocked. It can only be unlocked after the node rewards are issued (10 hours). Each node can only stake once in each block distribution cycle. When

distributing RPG to the rewarded verification nodes, it will be done according to each node's RPG stake ratio.

- After the block is produced, the verification group will receive 14% of the total block reward. All nodes in the verification group will be rewarded according to the nodes' stake ratio.



08. Ecosystem Construction

08.1 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 and include without limitation the following proposals:

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

08.2 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.

08.3 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 the 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 reward distribution to the node.

08.4 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 it 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

08.5 Developers

The Foundation will regularly hold development or game contests and other activities to attract developers at an early stage. 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 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.

09. Governance Mechanism

09.1 Proposal Nodes Election

Proposal nodes are generated using the algorithm mechanism of VRF+BLS. The user or organization using Rangers Protocol applies for the proposal node election to the Foundation. After paying the deposit, they can participate in the election of the proposal node.

09.2 Stake Mechanism

To become a system node (proposal or verification), ecosystem users must stake tokens.

The stakes are divided into proposal node stakes, verification stakes, and certified developer stakes.

1. The proposal nodes' stake can only guarantee that users can become proposal nodes.
2. The verification nodes' stake can ensure that users are selected into the candidate verification node pool. However, the verification group is formed by the verification nodes randomly chosen from all the candidate node pools.
3. 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 voting, and then forfeit a certain degree of fines towards the staked tokens. Similarly, certified developers must ensure that there is no 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.

09.3 Slash 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.

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:

1. Proposal nodes

In the Block Rewards part, we mentioned that the block-producing proposal node alone receives 10.5% of the total block rewards. So, if the proposal node does not act or do evil, it will lose this part of the reward, unwise for proposal nodes.

2. 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.

09.4 Parameters Modifications

Most of the system's operations (such as annual interest rate and the proposal nodes' block generation time) are specified based on the operational experience of many blockchain projects and their characteristics. However, with the system operation, the community and applications are constantly changing. These parameters are no longer suitable for the new environment of the time. The Foundation can initiate a proposal to modify the system parameters. The community decides whether the parameter will be finally modified by voting.

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

Ranger Protocol Token Economy White Paper reflects our current thinking on the token economy. 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 protocol of the existing blockchain industry.

11. The Project
Team, Partners & Investors

11.1 Team

ZKSUN

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.

JIUZI

Cofounder. Master's degree at Southeast University. More than ten years of software development experience. Former Alibaba technologist. Former Ali Security Department device fingerprint data product leader. The former head of password security technology at Ali Security. Former commercial, public chain architect.

JADE

Cofounder. Former core developer of Ubisoft Entertainment involved in projects such as Assassin's Creed and Prince of Persia. Independent Game Award Winner at Cologne Game Show, Germany. Thirteen years of game development experience. Dedicated to developing and publicizing blockchain technology, the token economy in gaming, and the entertainment industry. Founder of MIXMARVEL.

MARY

Cofounder. Masters degree with merit at the University of Leicester, United Kingdom. Worked in the world's leading Fortune 500 Company. Eight years of entrepreneurial experience. Founder of China's first Entertainment. Publishing Platform incubated by InnoSpace. An active investor in the internet industry. Cofounder of MIXMARVEL.

NICOLAS

BD Head. Graduated from Fudan University Law School. Has several years of experience in corporate services. Serves MixMarvel since 2018. Native speaker of Italian, English, and Chinese.

ALINA

Marketing Head. Bachelor's in advertising, Fudan University. Established an external visual image for dozens of companies and has several years of market experience in the software service industry. Native speaker of Russian, English, and Chinese.

GIOVANNA

Head of R&D Center. Ph.D. in Astrophysics from the University of Western Australia. Eighteen years of experience as consultant and researcher in data science and predictive models for various engineering and science applications. Designer of smart systems for data acquisition across different platforms, data mining, and implementation of artificial intelligence. Worked for several MNCs across three continents, always seeks the next technological breakthrough.

ARINA

Product Manager. Master's Degree in International Business at the Plekhanov Russian University of Economics. Internship in Cologne Business School in Germany. Qualification upgrade as Product Manager at Internet Initiatives Development Fund. 4 years of working experience as Product Manager in Web-Development in Electronic Commerce.

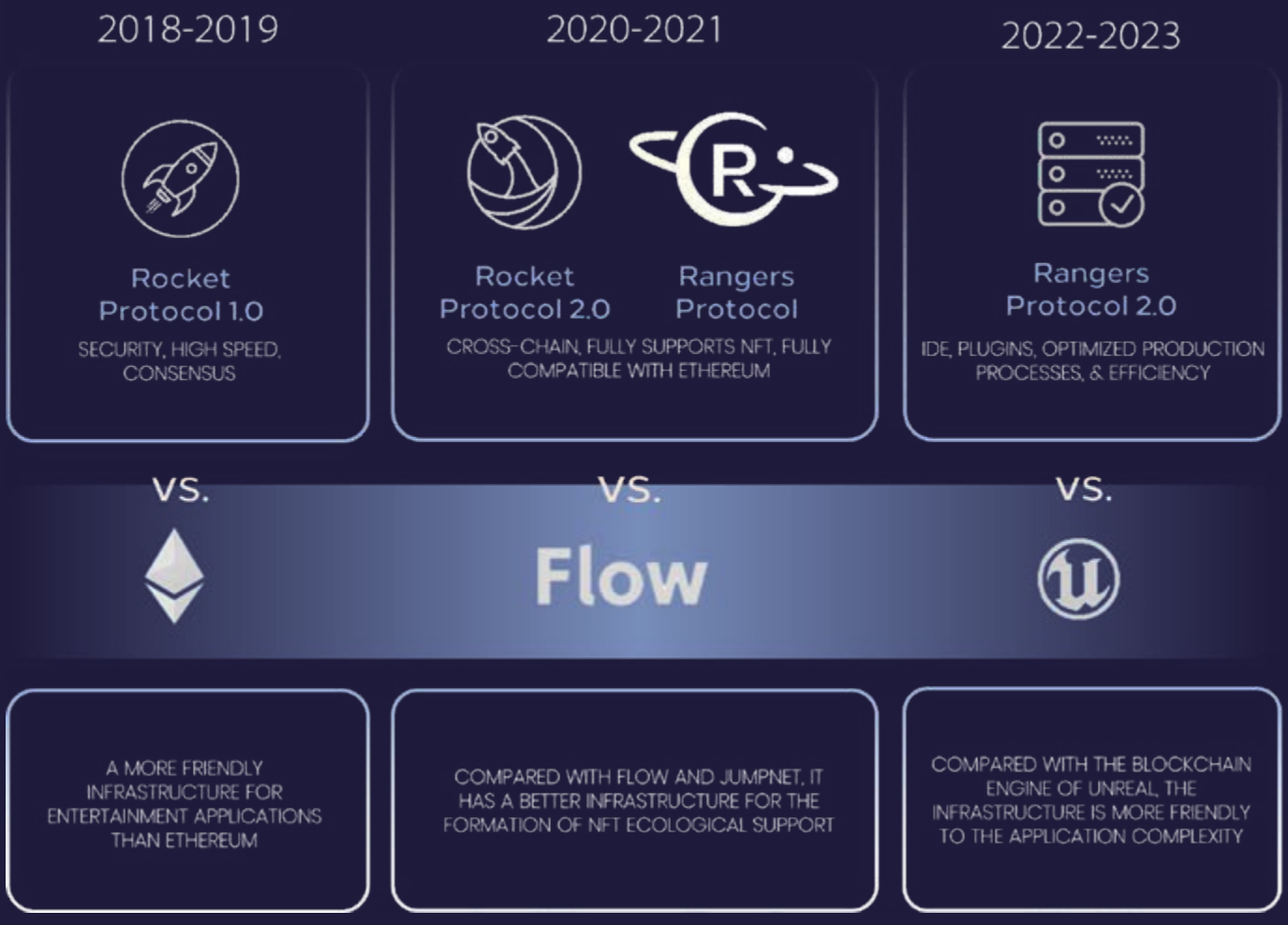
11.2 Partners

11.3 Investors

12. The Project
Roadmap

12.1 Rangers Protocol Tech Roadmap

Rangers Potocol's core positioning is to support the blockchain infrastructure of NFT and complex applications professionally. Rangers Potocol's long-term goal is to become a blockchain infrastructure that is friendly to decentralized application developers and users. Rangers Potocol'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).



12.2 Rangers Protocol Tech Roadmap

	Rangers Engine			Rangers Connector		
	Milestone	Target	Key Features	Self-Consensus Algorithm	Node Openness	Key Features
2021 Q1	Compatible with Ethereum NFT	Support Rangers Protocol-based dapp development	1. VRF+BLS consensus mechanisms 2. EVM-based smart contract system 3. NFT protocol stack	Multi-signature	Unable to join and leave freely	1. Average security 2. Limited multi-signatures amount 3. Fast consensus
2021 Q2	Compatible with Ethereum EVM	Support the existing Ethereum dapps to run on Rangers Protocol	1. New Rangers Protocol SDK 2. Compatible with the Ethereum SDK interface 3. Launch of Rangers Protocol/ Ethereum switch	Upgrade to PoW consensus	Free to join and leave	1. High security 2. Unlimited number of nodes 3. Slow consensus
2021 Q3	Cross-chain asset solution based on distributed signature	Support existing Ethereum assets to circulate in Rangers Protocol	1. Rangers Connector Launch 2. ERC-20 assets circulation plan 3. ERC-721 assets circulation plan	Upgrade to Rangers Connector's VRF+TSS (ECDSA) consensus	Free to join and leave	1. Extreme security 2. Unlimited number of nodes 3. Fast consensus
2021 Q4	EVM enhancement, Rangers Connector functions enhancement	Extend the Solidity syntax to improve the efficiency of vertical field development	1. NFT protocol syntax 2. DeFi protocol syntax 3. Cross-chain transfer of contracts	Upgrade to a Secure Multi-Party Computation Chain based on VRF+TSS (ECDSA)	Free to join and leave	1. High security 2. Fast consensus 3. High scalability 4. Unlimited number of nodes
2022 Q1	IDE launch	Support complex applications, maximize developer efficiency	1. IDE plugin 2. Smart contract compiler and debugger			
2022 Q2	Sub-chain plan launch	Support developers to publish sub-chains heterogeneous to Rangers Engine	1. Customizable basic components of the sub-chains 2. Customizable tokens and governance of sub-chains 3. Nodes and communities that can share the parent chain			