



LAYER2 TOKEN SWAP PROTOCOL BASED ON RHN-ROLLUP

L2 Lab
dev@l2lab.org

November 2, 2020



CONTENTS

Introduction-----	4
Mission-----	4
Feature-----	5
1. RhinoSwap Decentralized Swap Protocol-----	6
1.1 RhinoSwap system framework-----	6
1.2 RhinoSwap state tree-----	8
1.3 Deposit-----	8
1.4 Withdrawal (Withdraw)-----	9
1.5 Transfer (Transfer)-----	10
1.6 Increase Liquidity (Create Liquidity)-----	12
1.7 Reduce Liquidity (Remove Liquidity)-----	13
1.8 Swap transaction-----	14
1.9 Withdraw Liquidity-----	15
2. RhinoSwap protocol-----	16
3. RHN token economics-----	18
3.1 Economic model-----	18
3.2 Currency mining-----	18
3.3 destroy-----	19
3.4 Initial liquidity-----	19

3.5 Distribution mechanism----- 20

4. Milestones----- 21

2021 Q2----- 21

2021 Q2-Q3----- 21

2021 Q4----- 21

2022----- 21

5. RhinoSwap issuance unit----- 22

6. Whitelisted Exchanges----- 23

7. Plan after Binance Listing----- 24

Introduction

RhinoSwap is a cross-chain aggregation protocol incubated by the Rhino Labs team. RhinoSwap's mission is to provide users with cryptocurrency-based financial services, allowing various crypto assets to be exchanged in its decentralized wallet. In addition, it also provides "cross-chain exchange" to realize asset settlement in different networks without considering the limitations of typical blockchain networks. With the vigorous development of decentralized financial protocols (DeFi) and the increasing maturity of open financial markets such as lending, exchange, and derivatives, we hope to use RhinoSwap, combined with decentralized wallets, to create a one-stop aggregation exchange platform for developers. Provide a more free and open trading environment with users.

Mission

The innovation of DeFi has brought many practical applications to the industry and promoted the development of open finance. Decentralized exchange (DEX) is a notable example. With the participation and surge of consumers, it has gradually been recognized by the market. The total pledge value of the Ethereum DeFi project has exceeded US\$60 billion (DeBank data). However, network congestion and poor scalability have led to high transaction fees. With the emergence of various Layer 2 solutions and the efforts of some side chains such as BSC and HECO, investors now have more choices. However, the barriers between blockchains still restrict the use of assets, and RhinoSwap helps to deal with these restrictions.

In order to provide a more efficient and simpler trading method, we compare well-known exchanges on different chains to find the most effective transaction rate

for users. In addition, we connect different blockchain networks through cross-chain protocols, and allow users to freely exchange assets without considering network barriers.

Feature

No permission, anti-censorship: In any environment, anyone can access and use without permission, and does not need to pass any KYC review.

Liquidity aggregation: Users can directly access the liquidity of multiple DEXs on the corresponding network at one time through decentralized wallets, and obtain the highest quality and effective transaction prices.

Cross-chain transaction: Build a cross-chain transaction pool based on mature/potential cross-chain solutions in the market, allowing users to freely trade between multi-chain assets.

Community-driven: Innovative design based on the issuance and economic model of RhinoSwap Token will eventually achieve decentralized governance and community-driven development.

1. RhinoSwap Decentralized Swap Protocol

This project implements RhinoSwap, a Layer-2 AMM decentralized transaction protocol based on RHN-Rollup technology. It implements all the functions of uniswap on Layer-2, and realizes real-time transactions while ensuring the core value of decentralized transactions. The Uniswap TPS (the number of transactions that can be processed per second) has been increased by multiple orders of magnitude, and the transaction process hardly consumes any gas fees.

1.1 RhinoSwap system framework

The RhinoSwap system consists of on-chain smart contracts, off-chain RhinoSwap Server, zero-knowledge proof system and front-end user interface.

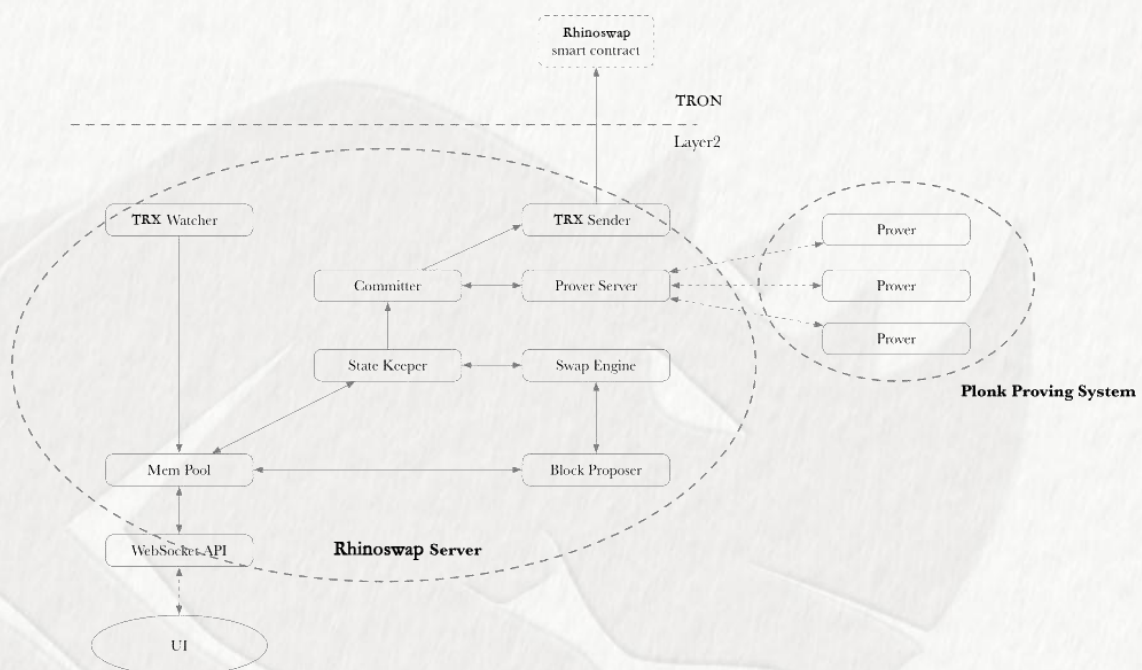


Fig. 1. System architecture

RHINOSWAP SMART CONTRACT RhinoSwap will deploy a series of smart contracts on the TRON blockchain to store the tokens deposited by users. At the same

time, it is necessary to record and verify Layer-2 status updates and related proofs, which connect on-chain and off-chain. The key hub.

RHINOSWAP LAYER-2 SERVER RhinoSwap server is a module that actually processes all transactions off-chain. The RhinoSwap server can interact with users through the WebSocket interface and can also monitor transactions on the Ethereum blockchain. All legitimate transaction requests will be placed in the RhinoSwap memory pool,

Swap Engine is ultimately responsible for processing. The transaction types in the memory pool are the same as all the operation types of Uniswap in the previous section. The Block proposer rolls up the transaction, generates a new block, and the State Keeper updates the state of all tokens in Layer-2. The State Keeper will send the state to the Committer, which is responsible for communicating with the Prove server, obtaining the proof of the corresponding transaction, and finally sending the state and the corresponding SNARK proof to the RhinoSwap smart contract on the chain through the Ethereum sender.

PLONK ZERO-KNOWLEDGE PROOF SYSTEM RhinoSwap's zero-knowledge proof system adopts a distributed architecture and uses the latest zero-knowledge proof algorithm PLONK[6] to generate proof. Prove server supports multiple Prover. Multiple Prover actively inquires the proof task in the Prove server, generates the proof and sends it back to the Prove server. The global trust setup of PLONK only needs to be generated once, and the application of the circuit scale within a certain range

Reusable, which greatly reduces the threshold for the use of zero-knowledge proof.

1.2 RhinoSwap state tree

The status tree of the RhinoSwap system records the balance status of all accounts in the current system. The state tree of RhinoSwap is a Merkel tree with a height of 34. The child nodes of the root node Root are all account nodes (layer 24) in the system. There are two types of account nodes:

- Ordinary account node, used to record the status of all Tokens in the account. Ordinary account nodes can have any number of leaf nodes (10 levels), and each leaf node represents a type of Token and its quantity; Token types under the same account cannot be repeated;

- Pair account node, used to record the status of a certain transaction pair fund pool in RhinoSwap. The Pair account node only contains two leaf nodes, and each leaf node represents the balance and type of a Token in the fund pool.

The transaction process in RhinoSwap is actually the process of updating the state tree. The following describes all transaction types and corresponding status changes in RhinoSwap.

1.3 Deposit

Deposit refers to the process by which users deposit tokens on the Ethereum chain into the RhinoSwap contract so that they can be used in Layer-2. The Deposit operation is initiated by the user from the chain. When the RhinoSwap Server monitors the user's transaction of transferring the token to the RhinoSwap smart contract on the chain, it will update the status tree according to the transaction details. First, find the corresponding Account according to the account to which the transaction belongs, and update the status of the corresponding Token under the Account according to the amount of Deposit. If there is no leaf node corresponding to

the Token under the Account, you need to create the leaf node corresponding to the Token first, and then update the status. After the status update of the leaf node is completed, the hash of the root node will be updated accordingly.

The updated hash of the root node of the state tree will be sent to the RhinoSwap contract on the chain together with the SNARK proof of the Deposit transaction.

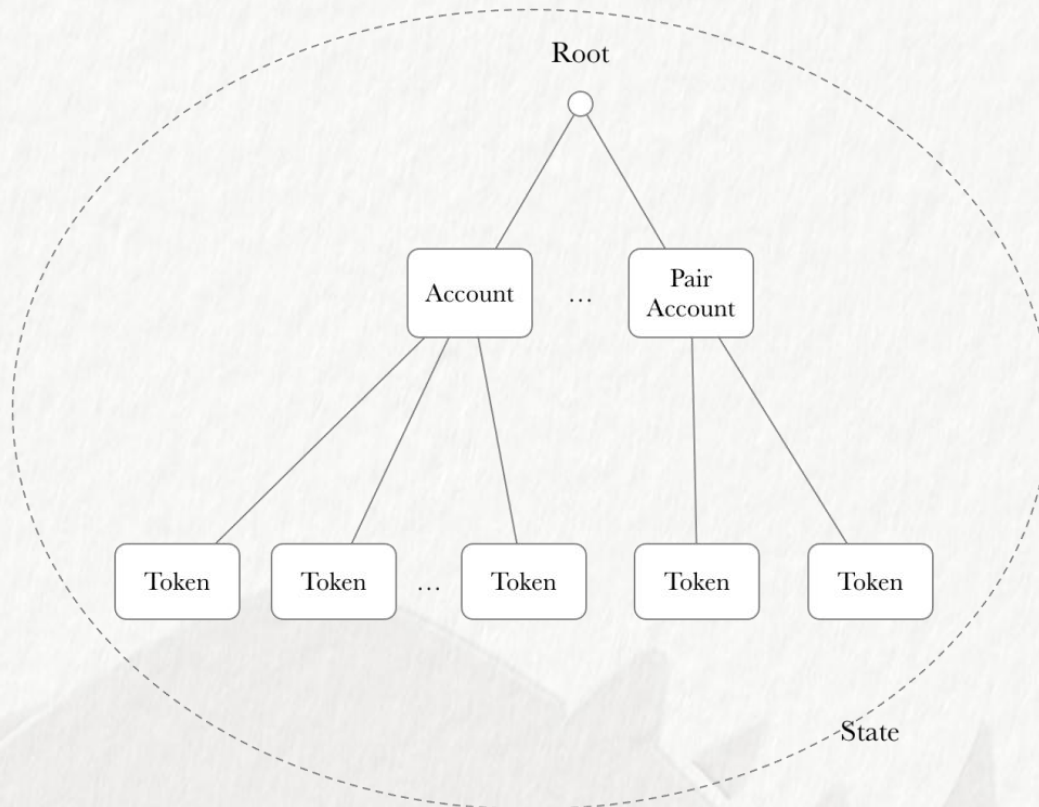


Fig. 2. State tree

1.4 Withdrawal (Withdraw)

Withdraw refers to the process in which the user withdraws the Token from Layer-2, unlocks it from the RhinoSwap contract, and sends it to the corresponding Layer-1 account. The Withdraw operation is initiated by the user from Layer-2. RhinoSwap server will update the status of the corresponding Token under the corresponding account after receiving the user's request to withdraw a certain Token, and hash the updated root node of the state tree with the Withdraw operation. The proof of the

application is sent to the RhinoSwap contract on the chain. After the contract is verified, the corresponding Token locked in the contract will be sent to the corresponding chain account.

1.5 Transfer (Transfer)

Transfer refers to the process in which a user sends a certain token to another user in RhinoSwap Layer-2. Transfer is initiated by the user on Layer-2. When RhinoSwap Server receives the Transfer request, it will find the corresponding sending and receiving account according to the request details, and update the status of the Token under the accounts of the sending and receiving parties according to the sent amount. The hash of the root node of the state tree will also be updated accordingly and sent to the contract on the RhinoSwap chain together with the SNARK certificate corresponding to the Transfer operation. Transfer will not change the status of the corresponding Token on the chain, because the Token is still locked in the RhinoSwap contract and has not been transferred on the chain.

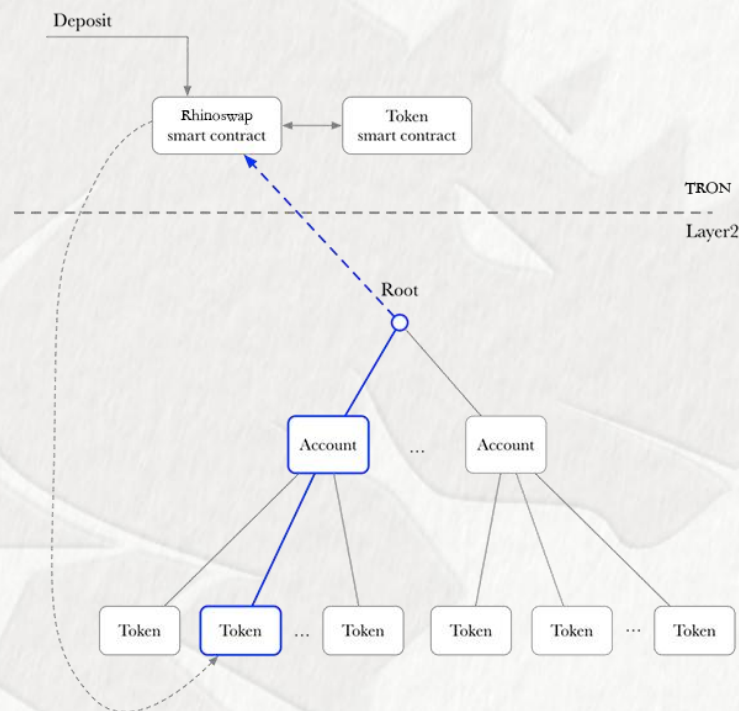


Fig. 3. Deposit

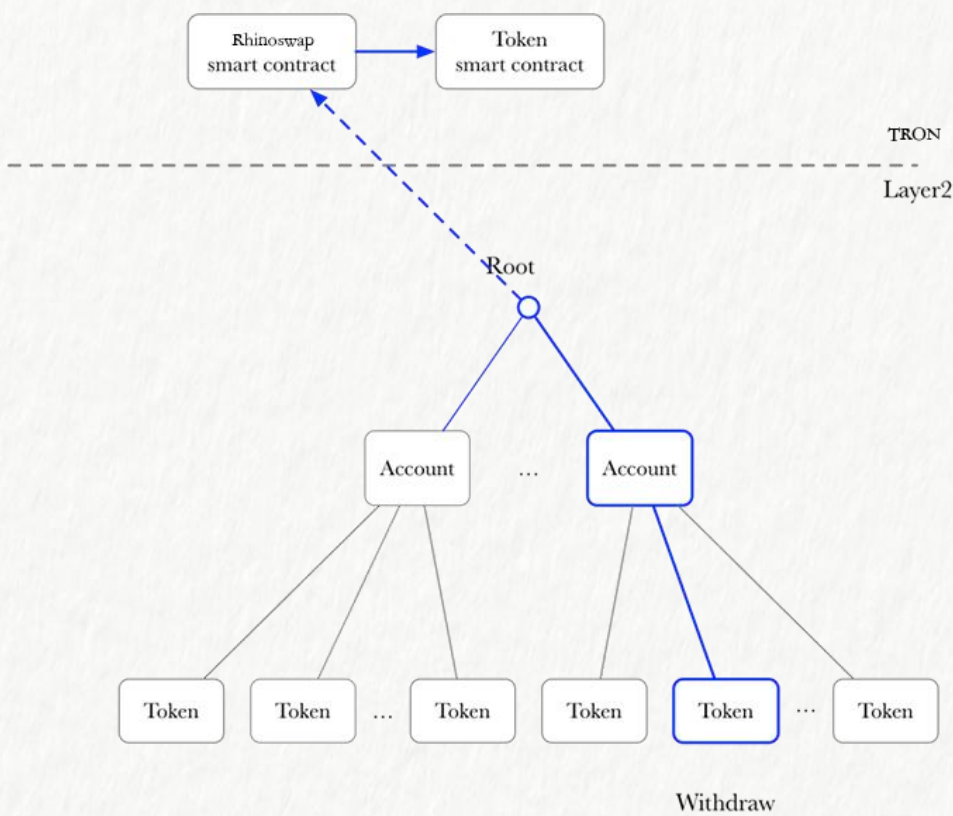


Fig. 4. Withdraw

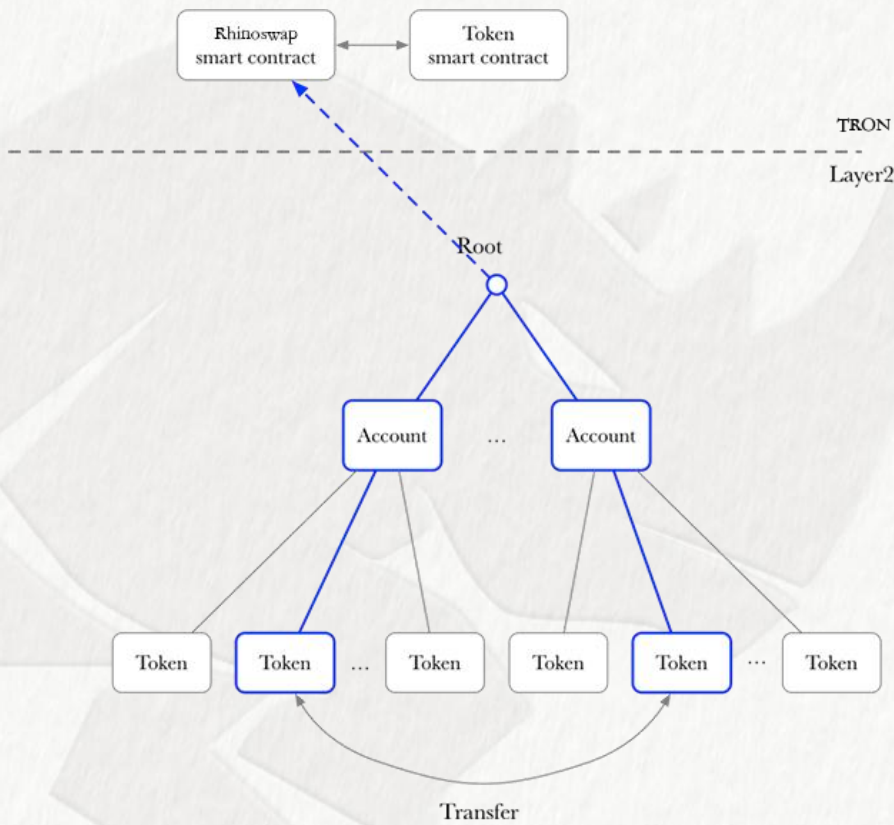


Fig. 5. Transfer

1.6 Increase Liquidity (Create Liquidity)

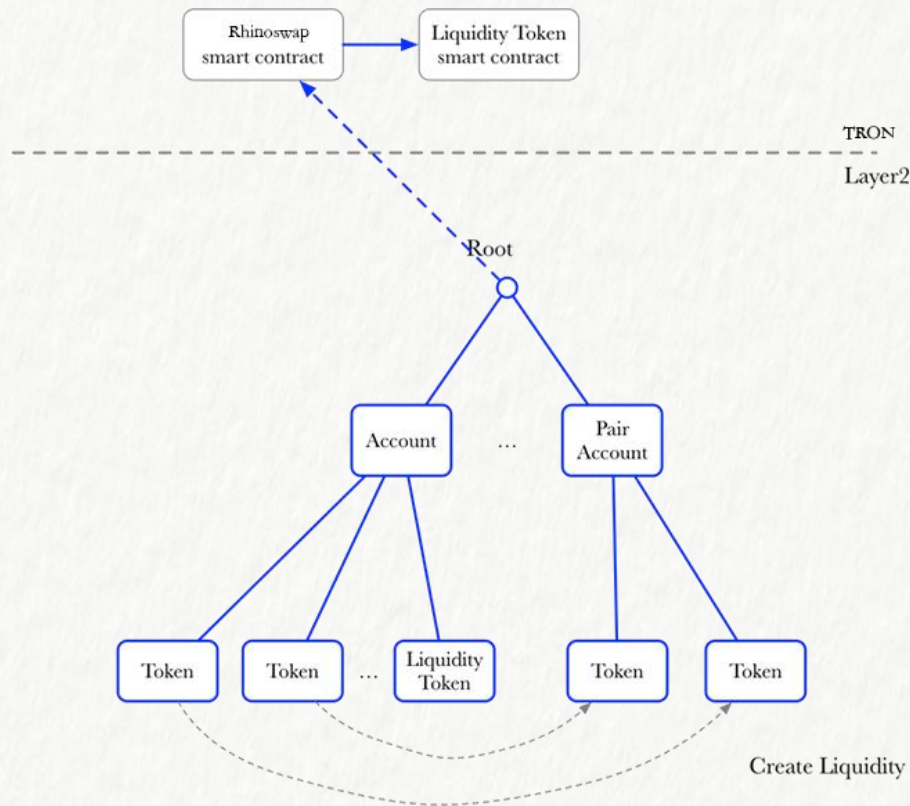


Fig. 6. Create Liquidity

Create liquidity refers to the user's operation to create or increase liquidity in Layer-2, and its definition is consistent with uniswap. Create liquidity is initiated by the user in Layer-2. When the RhinoSwap server receives a request from the user to create a pair of Token liquidity, it first needs to find the corresponding initiator Account and the Pair Account of the pair of Tokens (if the Pair Account does not exist, You need to create a Pair fund pool first); then transfer the two Tokens under the Account to the Pair Account according to the ratio specified by the AMM algorithm; at the same time, the system will calculate the number of LP Tokens that the user can obtain, and update the corresponding ones under the liquidity provider Account LP Token status. After all state updates are completed, the root node hash of the state tree will be sent to the RhinoSwap contract on the chain together with the proof corresponding to Create

Liquidity. The first created LP token requires the RhinoSwap contract to deploy the corresponding LP Token contract on the chain.

1.7 Reduce Liquidity (Remove Liquidity)

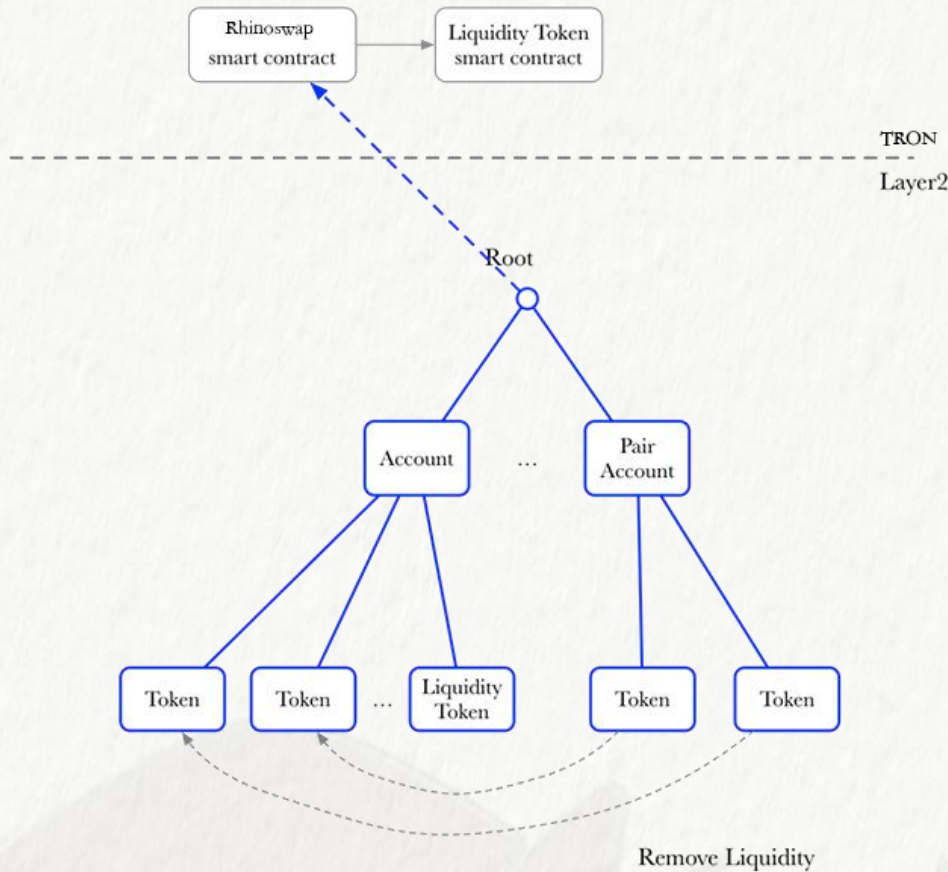


Fig. 7. Remove Liquidity

Remove Liquidity refers to the process in which the user destroys the LP Token from a certain Pair fund pool of Layer-2, and retrieves the corresponding proportion of the two Tokens in Layer-2. Remove Liquidity is initiated by the user in Layer-2. When RhinoSwap Server receives the user's Remove Liquidity request, it will first find the corresponding Account and destroy the corresponding number of Liquidity Tokens under the Account; then it will match the Liquidity Token to the two types of Tokens under the Pair Account. Transfer will destroy the Account of Liquidity Token in proportion. After the operation is completed, the state tree will be updated accordingly, and the root node hash and the proof of the corresponding Remove Liquidity

operation will be sent to the RhinoSwap contract on the chain.

1.8 Swap transaction

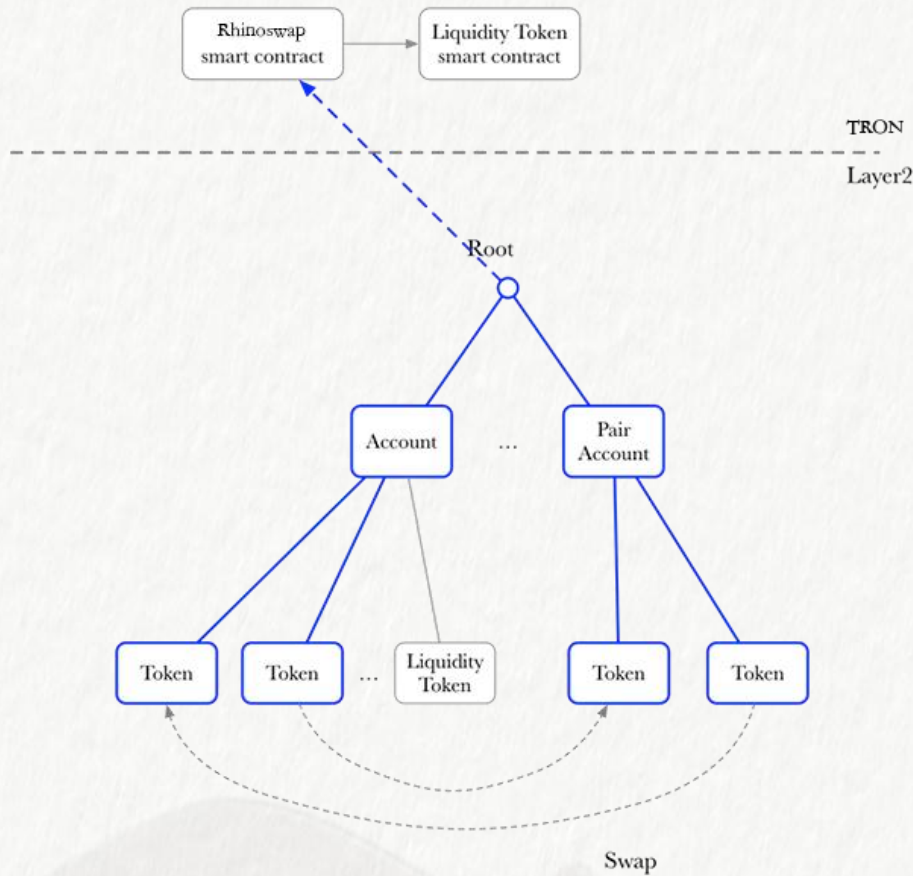


Fig. 8. Swap transaction

Swap refers to the process by which users complete transactions in the layer-2 fund pool. Assume that the user needs to perform a swap transaction in the fund pool containing TokenA-TokenB Pair Token. The user first sends the TokenA under his Account to the corresponding Pair Account from Layer-2, and RhinoSwap will calculate the number of TokenB that the user can obtain according to the AMM algorithm and send it to the user. The state tree is updated accordingly, and RhinoSwap Server will send the updated root node hash of the state tree and the proof corresponding to the Swap operation to the RhinoSwap contract on the chain. Swap transactions will not change the state of the token on the chain, because the token itself is still locked in the RhinoSwap contract.

1.9 Withdraw Liquidity

Withdraw Liquidity refers to the process by which the user withdraws the Liquidity Token from the Layer-2 account to Layer-1. The initiation process and status update of Withdraw Liquidity in Layer-2 are exactly the same as the above-mentioned ordinary Withdraw, but the results produced in Layer-1 are different. After the RhinoSwap contract receives the Withdraw Liquidity request, it will automatically trigger the mint operation of the Liquidity Token to create an additional Liquidity Token in Layer-1 and send it to the designated account.

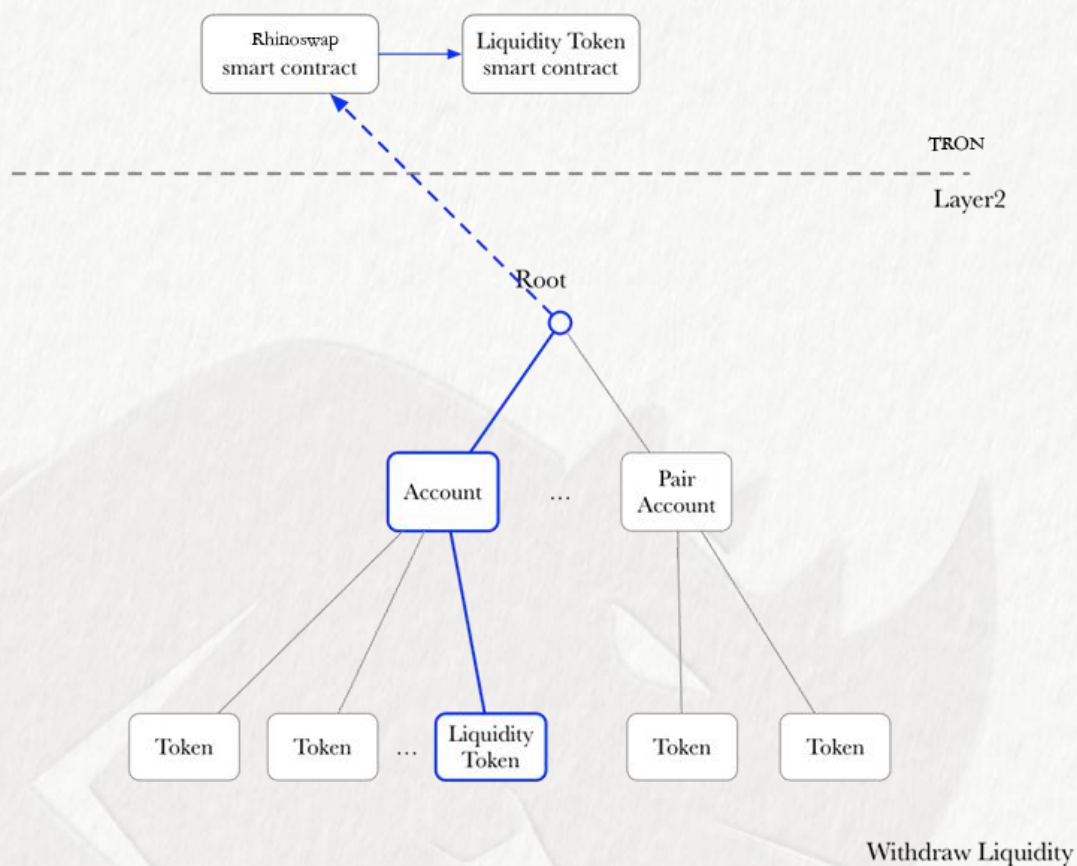


Fig. 9. Withdraw Liquidity

2. RhinoSwap protocol

Full name of the project: RhinoSwap

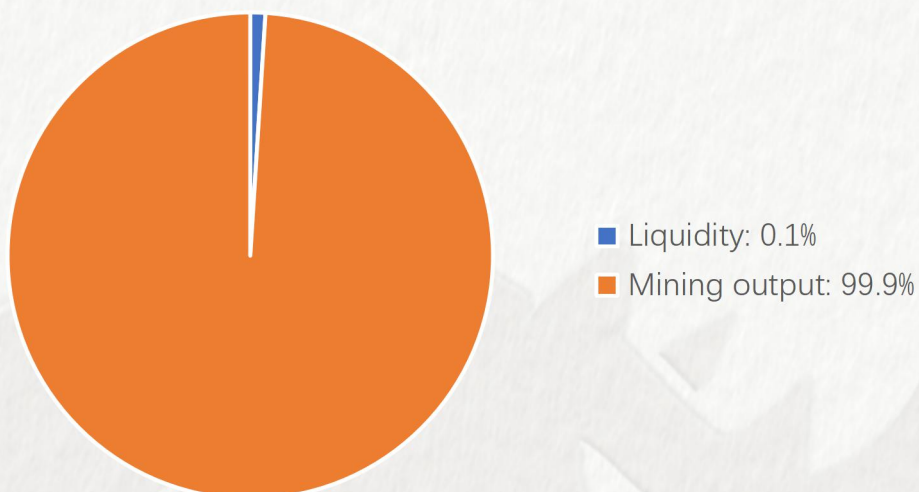
Token abbreviation: RHN

Circulation: 10 million

Liquidity: 0.1% (10,000)

Mining output: 99.9% (9,990,000)

Token Contract: To be determined



RHN is a governance token issued by RhinoSwap. It is an important medium to promote the development of RhinoSwap network. Based on the economic model of RhinoSwap, through the community governance mechanism of tokens, all participants are encouraged to invest in the maintenance and development of the overall ecological network.

RHN TOKEN USES TWO SIMPLE FUNCTIONS: transaction tax deduction, automatic market making

TAX DEDUCTION PER TRANSACTION (5%)

- 2% of the creation node dividend
- 2% enter the ecological construction address
- 1% enter the Rhino Foundation

AUTOMATIC MARKET MAKING

All USDT participating in exchange mining will automatically buy RHN in RhinoSwap to increase the price of the currency

3. RHN token economics

3.1 Economic model

In RhinoSwap's economic model, there are two ways to earn RHN. First, participate in the destruction and mining of RHN. Second, you can obtain RHN through DEX transactions through RhinoSwap.

RHN has three main uses:

Member rights: RHN holders can receive interest and transaction discounts allocated by the RhinoSwap Treasury.

Community governance: Users can participate in community governance by staking RHN to initiate proposals and participate in voting.

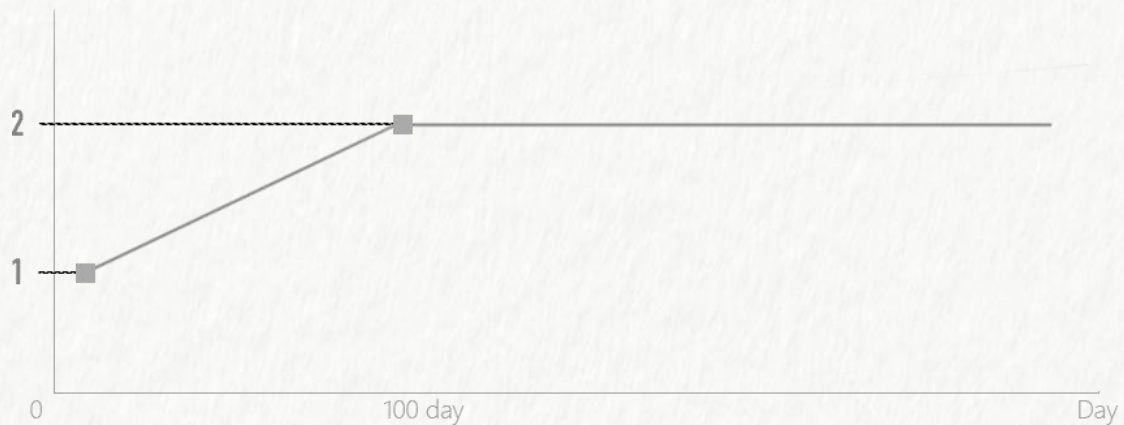
Community Alliance: Different communities obtain RHN computing power through pledge and destruction of their community tokens, and participate in RhinoSwap mining.

On the other hand, all transaction fees of RhinoSwap will be used to repurchase RHN on the open market on a regular basis, and will be distributed proportionally to RHN's equity holders and the development committee.

3.2 Currency mining

RhinoSwap community members obtain personal computing power by exchange 100USDT+ equivalent community tokens, and at the same time, calculate the weighted computing power according to the time factor of the pledge.

TIMEFACTOR=1+1%N



$$\text{PERSONAL POWER} = (100 + 100)N * \text{TIMEFACTOR}$$

That is, 10 days after the start of currency exchange mining, A has exchanged 200UST+ equivalent community tokens (for example, the Falari community needs to provide 200USDT F1), and his personal computing power is

$$(200 + 200) * (1 + 1\% * 10) = 440$$

where RhinoSwap will equally distribute the current block output RHN according to each person's capacity and the current overall network capacity

$$\text{Personal mining} = (\text{Personal Power} / \text{network Power}) * \text{Current Production}$$

3.3 destroy

Participate in exchange mining to obtain USDT automatically buy RHN in the RHN/USDT trading pair of RhinoSwap, and destroy the RHN obtained by buying; the automatic pull mechanism ensures that the price of RHN rises rapidly

At the same time, according to the final destruction to 500,000, it will no longer be destroyed; creating the scarcity value of RHN

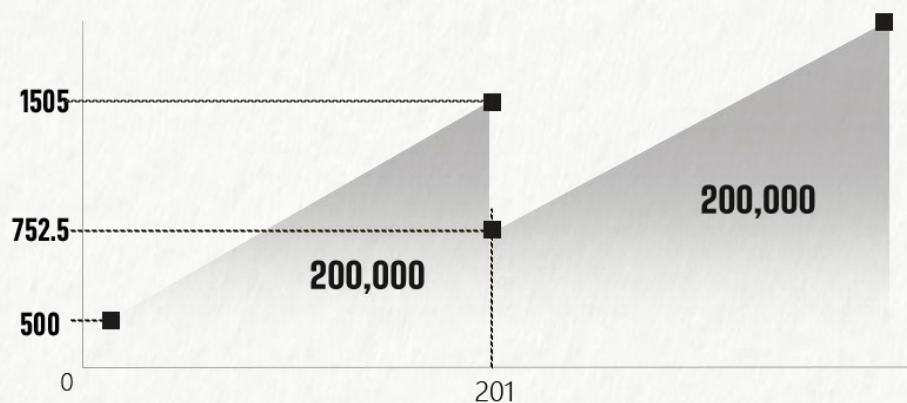
3.4 Initial liquidity

Early RHN added a liquidity pool, corresponding to 10,000 USDT, 1:1 equivalent sale;

at the same time, LPs that add a liquidity pool will automatically enter the lock-up state

3.5 Distribution mechanism

The total amount of RHN issuance is capped at 10,000,000 pieces, without any pre-mining and private placement links. 100% through the destruction of mining output



DESTROY MINING

Get 500 RHN on the same day, and the output will automatically increase by 5 every day

$$DAILY\ CAPACITY = 500 + 5 * DAYS$$

ICE AGE: APPROXIMATELY 5.79 MILLION TRON BLOCKS (APPROXIMATELY 29 WEEKS)

When the number of mined coins reaches 200,000 , the output will be automatically halved. The first halving will occur 201 days after RhinoSwap is turned on. At this time, RHN has initially established a consensus.

4. Milestones

2021 Q2

Mainnet is online

RhinoSwap is online

Release Litepaper V1

2021 Q2-Q3

RHN Hub is launched, providing cross-chain transaction services

Support ETH, BSC cross-chain exchange

RHN Version 1 released

2021 Q4

Start DAO Version 1

Complete Layer2 version development and deployment

Completed RHN Hub cross-Layer2 development

2022

Release V2, support real-time inquiry and pending orders



Release cross-chain 2.0

Start DAO Version 2

RHN network released

5. RhinoSwap issuance unit

RHINO UN LIMITED. (Registration Number: 10738792) is registered in England and Wales and issued by Cardiff Administration for Industry and commerce. Its businesses include blockchain underlying technology research and development, token economic model design, blockchain application technology development, digital asset management, digital asset M & A, industry consulting, etc. It aims to use blockchain technology to enable physical enterprises to promote industrial upgrading, and to promote the digital circulation of assets of enterprises and industries by combining assets with digital token.

	CS01 (ef)
Companies House	
Confirmation Statement	
Company Name: RHINO UN LIMITED	
Company Number: 10738792	
Received for filing in Electronic Format on the: 30/04/2021	
	
XA38970R	
Company Name: RHINO UN LIMITED	
Company Number: 10738792	
Confirmation Statement date: 24/04/2021	
Electronically filed document for Company Number: 10738792	

6. Whitelisted Exchanges

Half of the revenue of community operators will be used for including community construction, media promotion, technical maintenance, exchange listings, etc.

Apply for **Mxc** after tokens holder address > **25,000**

Apply for **Coinw** after tokens holder address > **50,000**

Apply for **ZB** after tokens holder address > **75,000**

Apply for **Gate** after tokens holder address > **100,000**

Apply for **Okex** after tokens holder address > **150,000**

Apply for **Huobi** after tokens holder address > **200,000**

Apply for **Binance** after tokens holder address > **300,000**

7. Plan after Binance Listing

NFTs: If technically achievable, we hope issue 100 NFT tokens, which will be obtained through auctions. Each NFT token will always receive 1% of the operating income of the RHN community. This may be the first truly decentralized company in global history.

Other DeFi: We envisioned many interesting and amazing plans, Will be rolled out gradually.

The end

By RHN community

operators