# ZKSpace: a Full-Featured Layer2 Protocol based on ZK-Rollups

L2 Labs
November 20, 2021

## 1. Introduction

Since 2019, decentralized finance (DeFi) has grown at an exponential rate. Blockchain developers, based on Ethereum (ETH) and top public chains, have created a series of applications, such as crypto exchange, mortgage loan, stablecoin, insurance, oracle machine, and games, forming a more complete decentralized financial ecosystem. As blockchain technology development gets prosperous and related applications develop and come into use, increasing new users start to know more about blockchain and participate in it. As well, the tolerant policy on global liquidity brings more unlimited financial resources. As shown on DefiLlama, now the Total Value Locked (TVL) of DeFi projects has exceeded 180 billion U.S. dollars, among which, the TVL on Ethereum ranks first and other public chains or sidechains, such as BSC, Terra, Solana, Fantom, and Matic, take up most of the residential market shares. These on-chain assets require fast, frictionless, trust-free, and real-time exchange services, and thereby leading to the rise of new exchange protocols, like Uniswap [1] and Sushiswap [2].

If DeFi has brought the initial users and funds for public chains, then GameFi and NFT give it more playability and collection value and make it more popular even outside the blockchain area, attracting a large amount of liquidity and fund from other areas. Because of the present performance limit of the blockchain, the exploration of the game field is still in its early stage. NFTs, not unexpectedly, have continued to be popular, with more and more influential persons in all walks of life focusing on, purchasing, and issuing NFTs, and most of the issuers and consumers have chosen Ethereum, which seems to be much decentralized and possesses a more mature ecosystem. OpenSea [3], the world's largest NFT trading platform, has its trading amount on Ethereum exceeding 3.4 billion U.S. dollars in August 2021, an increase of more than 10 times that of July. The CryptoPunks NFT collection is the most popular one, with its trading volume reaching about 202,000 ETH (approx. $800 million at that time) according to the current conversion rate.

All public chains with large market cap and user base, including Ethereum, have faced with the following common issues:

First, extremely high Gas fees of on-chain operations. Particularly, at its peak periods, a swap on Uniswap can even cost more than a hundred dollars, while an NFT transaction on OpenSea can cost hundreds of dollars, which is unacceptable to ordinary users and hinders new users from entry.

Second, limited by TPS, congestion will occur on public chains when there are surging users, which leads to long-time on-chain transactions and confirmation, with poor real-time

performance. And users, after long waiting, will fail their transactions which will be finished ahead by others, and then lose their patience and confidence.

ZK-Rollups [4] is a new Layer-2 scalability solution, compared with other solutions like Plasma, is of great advantages in security, cost, TPS, and usability, and thereby especially fitting to build Layer-2 service. Based on ZK-Rollups technology, L2 Labs has issued ZKSpace, a full-featured protocol of Layer-2, including DEX, payment, and NFT function, and it transfers all tokens (including protocols ERC20 and ERC721) onto Layer-2 using ZK-Rollups technology. The consistent state of Layer1 and Layer2 is guaranteed based on continuously generated zero-knowledge proofs, so as to make all token swaps, transfers, and NFT minting and trading on Layer 2, realizing real-time trading with no Gas fee (no need to wait for one-block confirmation). As well, it also has infinite scalability, getting rid of the limit on TPS and one-block confirmation on Ethereum. In addition, users can enjoy CEX and a smooth trading experience like traditional e-commerce platforms and can guarantee asset security of their own in real-time.

ZKSwap, a decentralized exchange based on ZK-Rollups under the ZKSpace protocol, has implemented the complete function of Uniswap on Layer2, reducing Gas fees to a tenth of a percent while ensuring the same security as Layer1. At present, there have been two updated ZKSwap mainnet versions, V1 and V2, achieving a series of remarkable milestones and running stably for nearly one year. ZKSquare, also realized based on Layer2, has also achieved more than 1 million transfers with the total amount of more than US$250,000 dollars within about 9 months from its issuing, reducing a lot of transaction costs for users.  In the coming days, the implementation of ZKSea will greatly optimize the users' experience when minting and trading NFTs and can return the pricing authority of NFT products to the artist and the market, which is unlimited for the high gas fee. We will also open the NFT minting interface to all NFT platforms.

The first version of ZKSea will possess the following functions:

1) Mining NFT with zero Gas fee on the Layer-2 network;
2) For functions of trading and transferring function with zero gas fee of NFT on layer-2, thousands of TPS can be reached theoretically;
3) NFT can be deposited and withdrawn between Ethereum Layer-1 and Layer-2 networks;
4) There is an NFT storefront, supporting free transactions between users on the Layer-2 network.

In the future, the ZKSpace protocol can further improve the Layer-2 performance and will issue more products to enhance the user experience, extending the ecosystem environment of Layer-2. L2 Labs team will also promote the multi-chains ecological strategy of "Layer-2 for all", and deployment is considered according to the ecological development of public chains like BSC and Solana. They will commit themselves to the R&D of the Layer-2 cross-chain bridge, so as to connect multiple chains' ecosystems, and then to provide a unified scalability service of Layer-2. Therefore, users can rapidly finish the cross-chain transactions at a low cost for their assets and then promote the prosperity of public chain ecosystems.

# 2 Technical Overview

## 2.1 Uniswap v1

Uniswap[5] is a set of decentralized trade protocols based on the “Constant Product” automated market marker mechanism, consisting of a series of smart contracts deployed on Ethereum. Users can create a liquidity pool by providing a certain percentage of Ethereum and any other ERC20 asset. Each funding pool stores a pair of assets and provides liquidity for transactions of both assets. In return, all liquidity providers will split 0.3% of the transaction volume as a liquidity provider fee. On Uniswap, the first liquidity provider needs to set the ratio of the two assets in the liquidity pool. The automated market maker algorithm will ensure that the product of the two assets before and after each transaction remains constant. Uniswap contains the following functional modules: creating a funding pool, generating liquidity tokens, adding liquidity, removing liquidity, and swapping tokens. Each liquidity provider (hereinafter referred to as LP) in the funding pool will obtain liquidity provider token (hereinafter referred to as LP Token) from the corresponding funding pool, representing the portion LP taken up in the current funding pool. LP Token is a kind of token in accordance with the ERC-20 standard, which can be transmitted without removing funding pool liquidity. Each funding pool has its corresponding LP Token. If there is a user making Swap transaction, token exchange with the whole funding pool will happen, that is, put the selected number of certain a token into funding pool, another token will be exchanged according to a constant product model. Token changes in this funding pool will be shared by all LPs, which comprise the funding pool, per the proportion.

## 2.2 Uniswap v2

Uniswap v1 realizes the basic AMM exchange center function but there still exist some problems. Because the contract is non-upgradable, to fix this problem, the development team has re-implemented a version, Uniswap v2 [6]. Uniswap v2 shares the same basic functions as Uniswap v1, but it also has some new features, including:

- It is possible to create trading pairs of two ERC-20 tokens directly, instead of using Ethereum as media for both as Uniswap v1;
- It is a more reasonable price oracle machine, which takes advantage of the randomness of the price of the previous transaction before the first transaction in the block to make the price hard to be manipulated;
- Flash Swap. Users can obtain the target tokens first and then finish Swap; or the tokens can be returned within a specified time to avoid triggering the Swap process, which means that users can borrow the tokens in the funding pool;
- The original 0.3% liquidity provider fee can be divided into two parts, of which 0.25% is still used to split by liquidity providers proportional to their contribution to liquidity reserves, and 0.05% is sent to the pre-set address as the Protocol Fee, which can be used for different purposes;
- These new features increase the availability of Uniswap, and the ZKSwap features included in ZKSpace described in this article are the same as Uniswap V2.

## 2.3 NFT

### 2.3.1 NFT Background

NFT is short for Non-Fungible Tokens, with irreplaceable and unique characteristics, which means that it can digitize some of the sole artworks or assets, such as a Beethoven's piece or a Van Gogh's painting.

Same with some mainstream crypto assets like Bitcoin (BTC) and Ether (ETH), NFT can be recorded in the blockchain, and it is accessible to anyone without being modified. But the difference between NFT and other mainstream crypto assets is that every NFT token is unique and indivisible. Upon you buy an NFT token, you acquire its rights of exclusiveness and actual assets usage. For example, if you buy an NFT weapon in a game, rights of display and usage will belong to you unconditionally, unless you voluntarily transfer it to other users; or if you buy an NFT art piece, you can acquire the rights of actual usage and copyright.

NFT is the only indivisible asset in the digital world. It can be minted, traded and can digitize assets from different domains, and can be used to anchor some physical goods in the real world. With the development of blockchain technology and the emergence of more NFT platforms and applications, more and more artists, celebrities, and institutions begin to enter the NFT field. Currently, the mainstream types of NFT include art, music, virtual world assets, game cards, collectibles, domain names, etc., which have been extended to all aspects of life.

### 2.3.2 NFT Protocol

NFT is essentially a technology protocol standard based on underlying blockchain in the process of asset digitization. Ethereum developers are soliciting opinions publicly, hoping to define a unified communication interface and establish a set of standards that can be followed, so that Ethereum developers can write smart contracts more smoothly. Therefore, a set of generic protocols called ERC (Ethereum Request for Comments) occur, among which, some widely used protocols are as follows:

(1) ERC-721 -- metadata structure of NFT token on Ethereum. It is the first standard representing Non-fungible digital assets proposed by Dieter Shirley in September 2017, and it is also the most commonly used token form in the NFT field. ERC-721 defines the minimum interface that smart contracts must implement to allow management, ownership, and trading of unique tokens. Under this standard, it is able to convert assets into sole and unique 256-bit meta-tokens, which can be tracked through smart contracts on the blockchain to be established.

(2) ERC-1155 – created by the Enjin team in June 2018, using a new way to define tokens. Items will be stored in a central smart contract and take up only bare space to distinguish each other. It can send multiple items in one single transaction, greatly improving the efficiency and being more convenient, and on the other hand, reducing the gas fee and network resource consumption.

(3) ERC-998 -- composable NFT, originally proposed by Matt Lockyer. This protocol can package different types of tokens (ERC-721 type tokens and ERC-20 type tokens) to enable combined transfer capabilities.

(4) ERC-420 -- originally proposed by PepeDapp. It can be used as a standard for digital transaction cards.

ERC-721 takes up the largest market share of NFT standard protocols, followed by ERC-1155. Developers can easily generate a set of similar NFT assets based on protocol standards. With the scalability of the NFT market and the development of blockchain technology, it can be believed that there will be more NFT standard protocols in the future to meet different users' needs.

# 3. Scalability Technology

## 3.1 Background

Ethereum network, the most active development platform in the blockchain world, has various DeFi protocols deployed. Those protocols inevitability lead to increasing network congestion and higher gas fees, and the situation is also becoming worse with the explosion of the NFT marketplace. Such terrible experiences, if without any improvement, will exert a negative influence on the Ethereum development.

Therefore, more and more blockchain researchers and developers are dedicated to researching underlying technology to improve the network status with all kinds of means.

Some technical solutions are for Layer-1, such as the sharding technology of ETH 2.0, which improves the block generation efficiency by modifying or optimizing the consensus network of the blockchain, thereby speeding up the block confirmation time to complete on-chain transactions.

Some technical solutions are for Layer-2. On the premise that the functions of Layer-1 are sufficiently simple, powerful, and stable, the calculations and operations originally on Layer-1 are carried out off the chain while ensuring the accuracy of these off-chain operations with cryptography technology.

However, from a long-term perspective, the Layer-2 based scalability technology solution will be more suitable for the healthy development of blockchain.

As the blockchain infrastructure is relatively clear, stable, and easy to maintain, imposing complex logic may make Layer-1 more and more fragile.

Therefore, concerning the development direction of the blockchain structure, Layer-1 should remain as unchanged as possible unless there is a major change, such as a breakthrough in cryptography technology leading to the modification of the cryptographic primitives used in the

underlying layer. Other complex logic and innovative applications should be placed on layer-2. Layer-1 and Layer-2 are complementary to each other.

Researchers have also gradually discovered this point, and Layer-2-based scalability solutions are emerging one after another. However, when putting the theory into practice, the developers realize that there are too many places to weigh the pros and cons to achieve expectations. For different application scenarios, they may have to make further compromises.

## 3.2 ZK-Rollups

So far, among Layer-2 scalability solutions, ZK-Rollups, Optimistic Rollup, Validium, and Plasma have caught most discussions.

**ZK-Rollups:** proposed by Ethereum researchers and characterized in that all computing processes are completed off-chain and stored on-chain. The plaintext data in the computing is sent to the on-chain contract in the form of call data, so as to reduce the storage cost. At the same time, the off-chain computing correctness is guaranteed by the zero-knowledge proof algorithm. With such designs, this solution can not only greatly increase TPS, but also reduce the cost of a single transaction.

**Optimistic Rollups:** consists of Optimistic Rollup (ORU) and Arbitrum Rollup (ARU). Both of them can ensure security through a challenge mechanism but in different ways. ORU is to challenge a transaction, that is, EVM will finish a whole challenged transaction, while ARU subdivides and regards the transaction process as orderly instructions one by one, and then after multiple rounds of interaction, finds out the abnormal one for a challenge, which make a very low verification cost. However, compared with ZK-Rollups, the security assumption of Optimistic Rollup is relatively poorer.

**Validium:** proposed by StarkWare and approved by Vitalik Buterin, and it was named so. It is characterized in that its computing process is completed off-chain and the computing correctness is guaranteed by zero-knowledge proof algorithm, the verification shall be finished on-chain and the final world state shall be stored on-chain. It should also be noted that, in this solution, the transaction data are also stored off-chain in order to achieve better scalability, and the trusted "Data Availability" Committee will provide underlying proof. Compared with the above-mentioned two solutions, this one loses a certain amount of data availability but does provide better data scalability. Therefore, this solution may be more favored in practice.

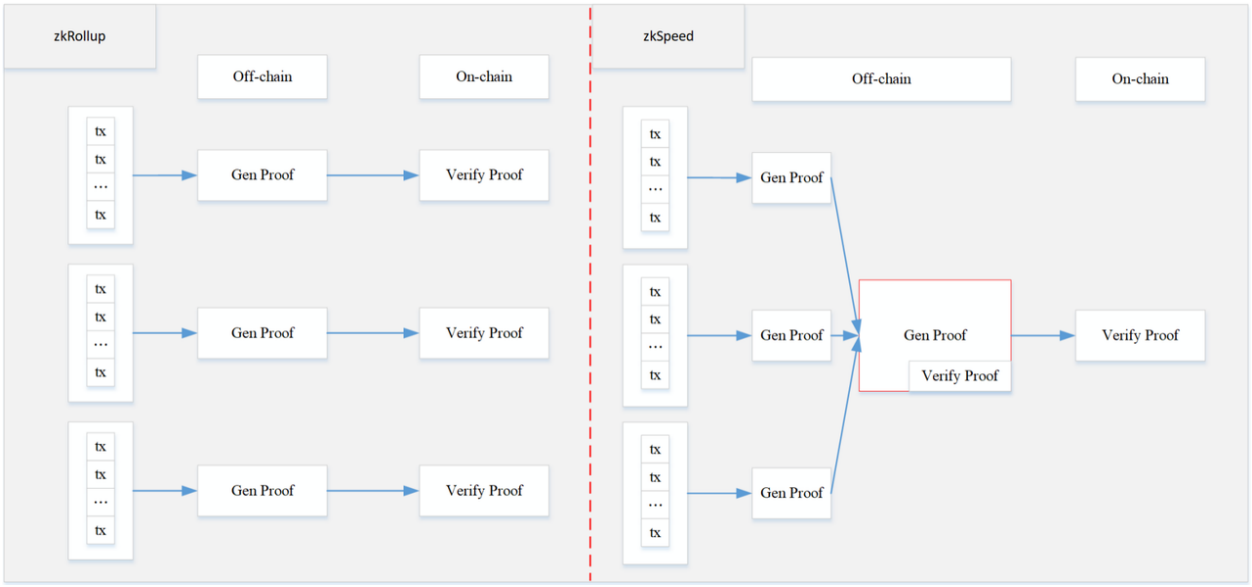
**Plasma:** proposed by Vitalik Buterin. Compared with the other three solutions, this solution, the earliest proposed one, is featured significantly. Its computing is finished off-chain and stored on-chain, and transaction data will be stored off-chain, which is easy to operate. Users can implement an error-proof to prove evil behaviors of operators to obtain rewards and punish such operators.

There is no doubt that only **ZK-Rollups** can provide the same security to our system as Layer-1, and this is why we choose it.

## 3.3 Aggregative proof

ZK-Rollups solution, based on the zero-knowledge proof algorithm, ensures that the changes in the world state caused by all transactions in a block are correct. Multiple transactions can be finished at one time to improve the system performance for the first time and bring higher TPS. However, due to the limited circuit scale, the improvement of this solution has not reached the expectation and is not enough to support the current volume on layer-2. Therefore, an additional technical protocol is needed for the overall performance improvement, which is Aggregative Proof.

Actually, Aggregative Proof has a very simple logic. As we all know, in the basic Layer-2 scalability solution, there is a corresponding validity proof for each block, and the proof is verified by the on-chain contract. At present, the average speed of block production on Ethereum is 15s. If the multiple proofs can be verified on-chain at one time, the cost shared in each transaction will be greatly cut down. The so-called Aggregative Proof solution is that, for the current state in which one proof is for one block, aggregate multiple proofs generated in a period of time or in a fixed number of blocks and verify these proofs of these blocks are valid using zero-knowledge proof (regarding the verification process as a circuit). In this way, only one on-chain verification is required for multiple block validity proofs. The schematic diagram of Aggregative Proof is shown as follows:



# 4.ZKSpace: Full-Featured Layer2 Protocol

This project has realized one Layer-2 full-featured protocol based on ZK-Rollups technology, supporting all token transactions on layer-2 and ensuring the consistent state of Layer-1 and Layer-2 through listing aggregation package on-chain, so as to maintain the same decentralization and security of the mainnet of public chains. Meanwhile, there is no need to wait for one-block confirmation on layer-1 for all token transactions, and it can update the TPS to a much greater level. And also, the Gas fee has been reduced as low as its one-tenths.
At present, we have developed three products, namely ZKSquare, ZKSwap, and ZKSea, including multiple functions like wallet, DEX, and NFT (Entrance to ZKSquare can be found in the ZKSwap wallet). Here is the specific realization of all kinds of products.

## 4.1 ZKSwap: Decentralized Swap Protocol

### 4.1.1 Systematic Architecture

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

### 4.1.2 ZKSwap Smart Contract

ZKSwap will deploy a series of smart contracts on Ethereum to store the tokens deposited by users while recording and verifying the Layer-2 status updates and related proof. Those smart contracts are the key hub connecting on-chain and off-chain.

### 4.1.3 ZKSwap Layer-2 Server

ZKSwap server is a module actually processing all transactions off-chain. It can interact with users through the WebSocket interface and monitor transactions on Ethereum. All legitimate transaction requests will be put into the ZKSwap memory pool and finally processed by Swap Engine. The transaction type in the memory pool is the same as all operation types on Uniswap mentioned in the previous section. Block Proposer executes the Rollup to the transaction, with new blocks generated, while State Keeper updates the state of all tokens on layer-2. State Keeper will send the updated state to Commiter, who is responsible for communicating with the Prove server to obtain corresponding transaction proof, and finally, send the state and SNARK proof to the on-chain ZKSwap smart contract through the Ethereum sender.

### 4.1.4 Plonk Zero-Knowledge Proof System

ZKSwap's zero-knowledge proof system adopts a distributed architecture and uses PLONK, the latest zero-knowledge proof, to generate a proof. Prove server supports multiple Provers, which means that if there are multiple Provers actively query the proof task in the Prove server and send it back to the prove server after generating the proof. The global trust setup of PLONK only needs to be generated once and all applications with circuit scale within a certain range can be reused, which makes it much easier to use zero-knowledge proof.

### 4.1.5 ZKSwap State Tree

The state tree of ZKSwap has recorded the balance of all accounts in the current system. It is a Merkel tree, with a height of 34. The child nodes of the Merkel Root are all account nodes in the system (24 layers). There are two types of account nodes:

- Ordinary account node, to record the state of all tokens in the account. An ordinary account node can contain any number of leaf nodes (10 levels), and each one represents a type of token and its amount. there can't be repeated token types within one account
- Pair account node, to record the state of a trading pair's funding pool on ZKSwap. The pair account node contains only two leaf nodes, with each one representing the balance and type of a token in the funding pool.

The transaction process on ZKSwap is essentially the process of updating the state tree. Based on this, ZKSwap V1 has realized all DEX functions including the deposit, withdrawal, transfer, and swap of tokens, and adding/removing/withdrawing liquidity. For state changes corresponding to each transaction type, refer to the Whitepaper of ZKSwap V1.

### 4.1.6 ZKSwap Token Scalability

In view of the limited circuit efficiency of ZKSwap V1, and its token volume cannot be scaled infinitely, then on ZKSwap V2, the function of unlimited token listing is added. Specific updating includes:

1) "Unlimited" token listing - When paying a certain amount of fee, users can list any volume of tokens independently and create a trading pair;

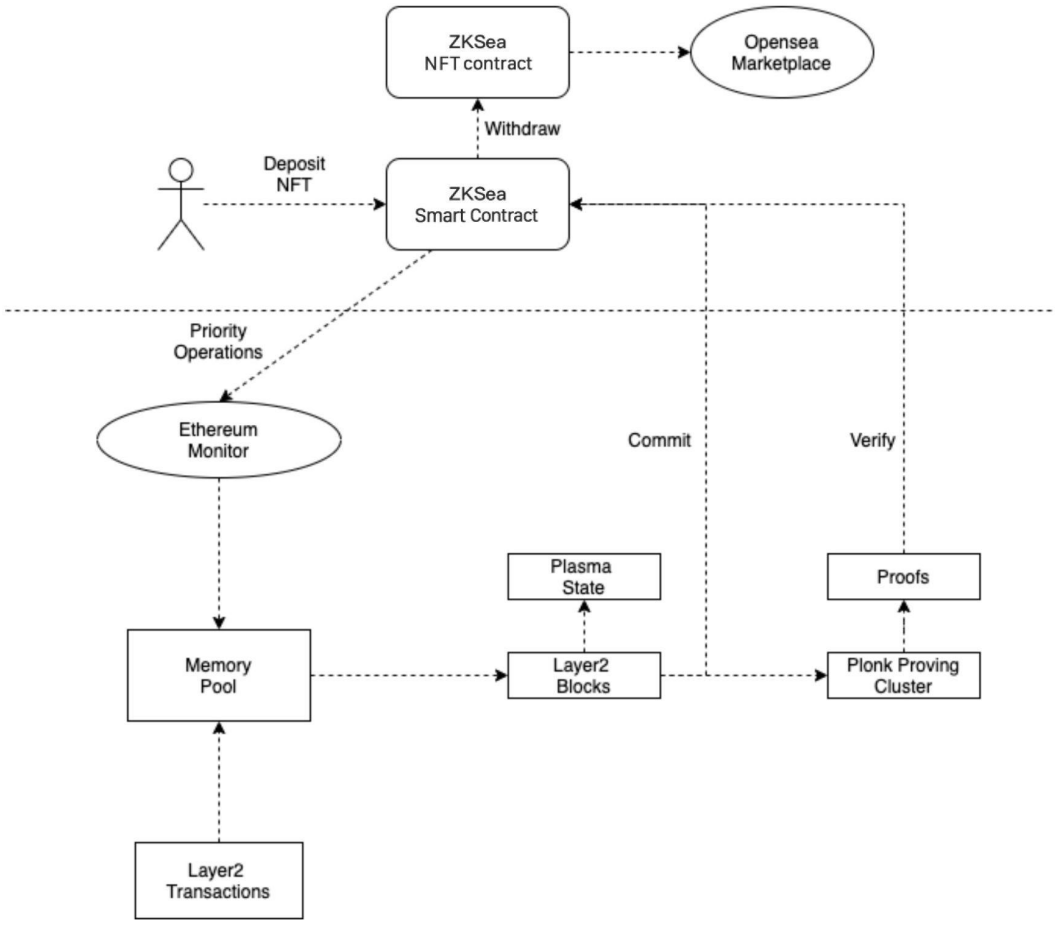
2) Optimization of circuit branches and improvement of circuit efficiency - supporting modification of one account and two balances;

3) Optimization of user's token withdrawal experience - coupling the withdrawing with the block verification and making it more flexible to accelerate withdrawing speed.

For detailed structure optimization of ZKSwap V2, refer to the Whitepaper of ZKSwap V2[9].

# 4.2 ZKSea: NFT Protocol of Layer-2

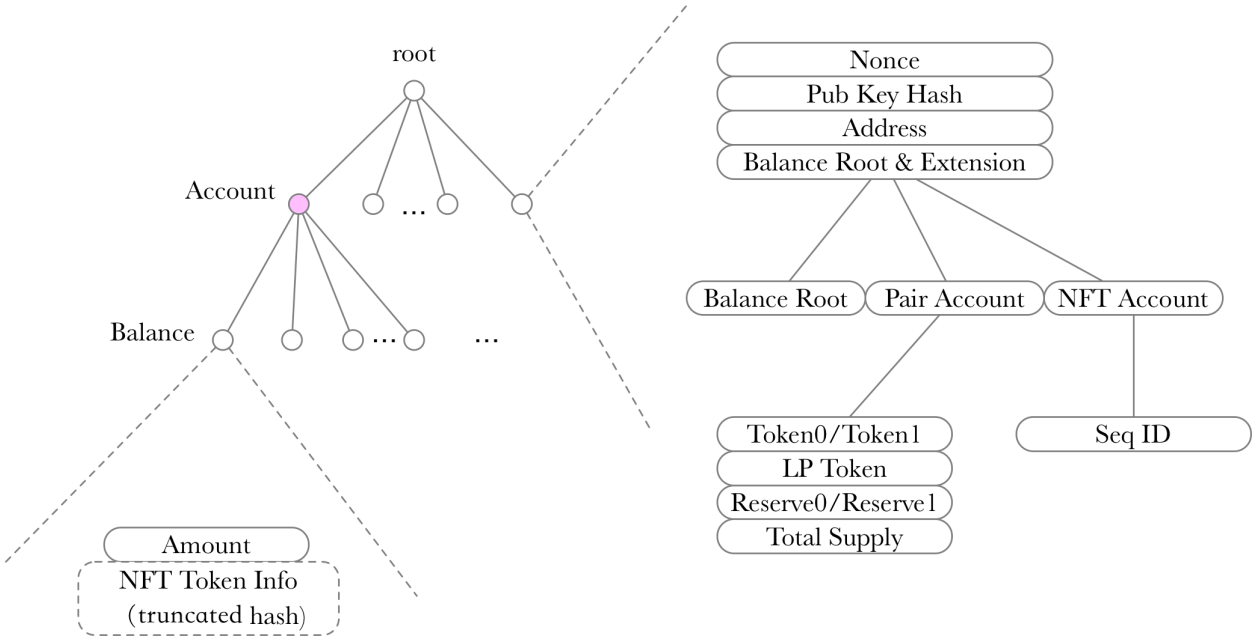
## 4.2.1 ZKSea System Architechture




## 4.2.2 NFT Model Design

Extend related information of NFT in the account information:

Seq ID – each Layer-2 account will publish one NFT, and there will be one more Seq ID.




The NFT information of an account consists of the following seven fields, no more than 756 bits:

(1) Global Token ID - NFT token ID global number, 64bit
(2) Creator - the founding account ID of NFT Token, 32bit
(3) NFT Seq ID – NFT sequence number of Layer-2 account, 32bit
(4) URI information - CID information of IPFS, CID V0, 32 bytes - 256bit
(5) Owner Account ID - Owner account number, 32bit
(6) Approved Account ID – account number of authorization objects (If is 0, the purchase account is not limited.)
(7) Approved Token ID – authorized Token number, 16bit
(8) Approved Token Amount – the price of NFT waiting for selling, 128bit

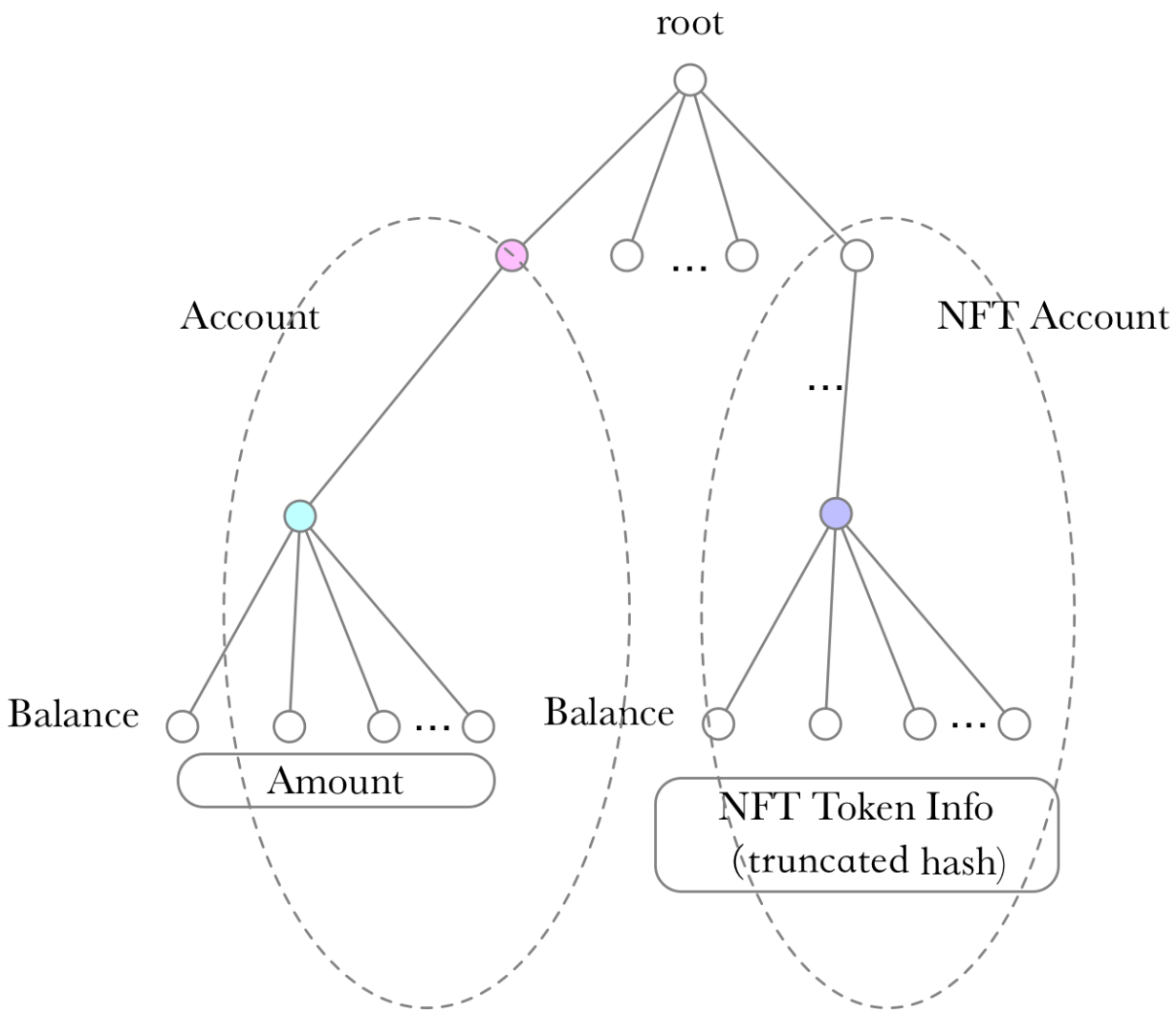
Layer-2 accounts, when creating NFT Token (Mint NFT), must determine NFT Seq ID, which equals to account.SeqID + 1. Global Token ID can be selected randomly on layer-2, only to ensure that a new account is created on an empty account. If the Approached-related information determines “purchase” information, any user can buy it at any price.

For all NFT created by a Layer-2 account, related information is stored on IPFS, with each NFT having its sole URI information.

Each NFT Token in the layer-2 account has two IDs: Global NFT Token ID and Creator + Seq ID.

Global NFT Token ID is the global sole indication.

Account, starting from 2^27, is reserved for storing NFT information:




### 4.2.3 NFT Operation Design

NFTs issued on Layer-2 are numbered uniformly (NFT Token ID) for management. All the NFT operations on Layer-2 shall be charged.

#### 4.2.3.1 Deposit NFT

The Deposit request initiated on Layer-1 can map the NFT of Layer-1 to Layer-2. For the Layer-1 NFT, ZKSea smart contract will transfer the NFT smart contract to create the corresponding NFT. All NFTs issued on Layer-2 are managed by the NFT smart contract.

Note: the Token ID of third-party NFTs deposited from Layer-1 accounts can be “assumed” not a random number, like some ordered value starting from 1 and less than 2^252. View popular NFTs:
https://etherscan.io/tokens-nft

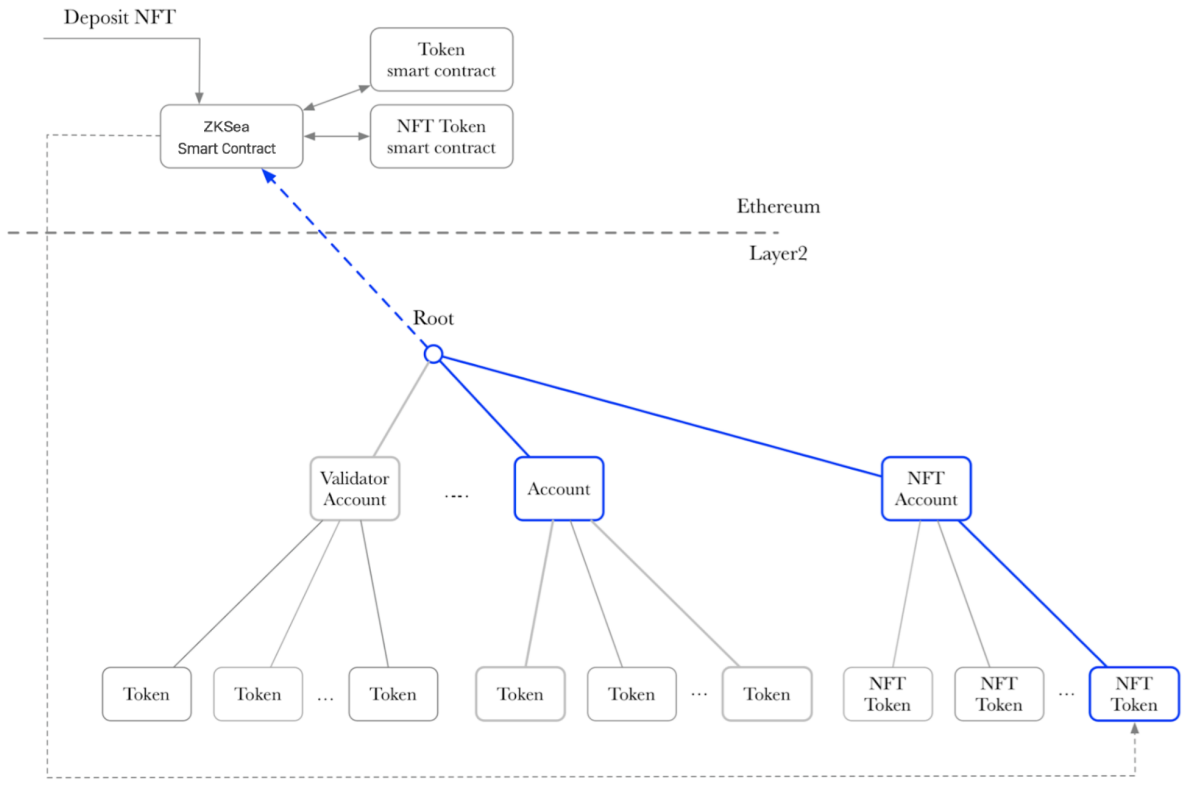
There are two cases for NFT deposits:

(1) Deposited by a third party.
(2) Issued on layer-2 and now withdrawn to Layer-1.

In the first case, only the corresponding Global NFT ID being created on layer-2 is enough. The specific information of the NFT is recorded by Layer-2.

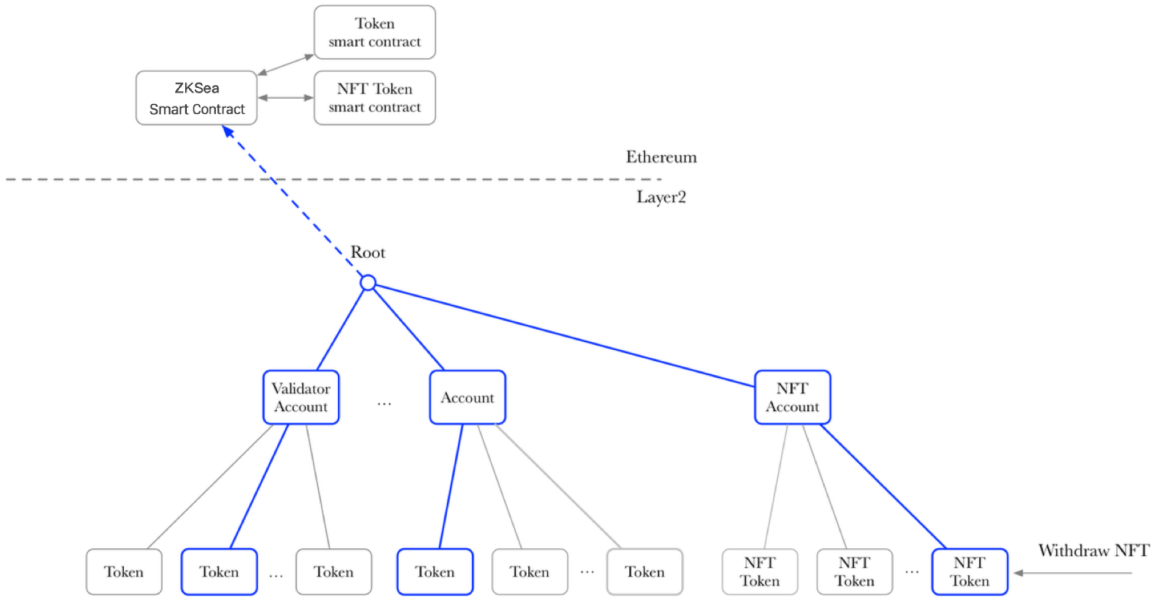
To respond to the deposit processing order on Layer-1, it can be synchronized between Layer-1 and Layer-2.

For the second case, specified NFT information shall be synchronized between Layer-1/Layer-2 (including Creator/Seq_id/URI/Owner). Details are shown as follows:



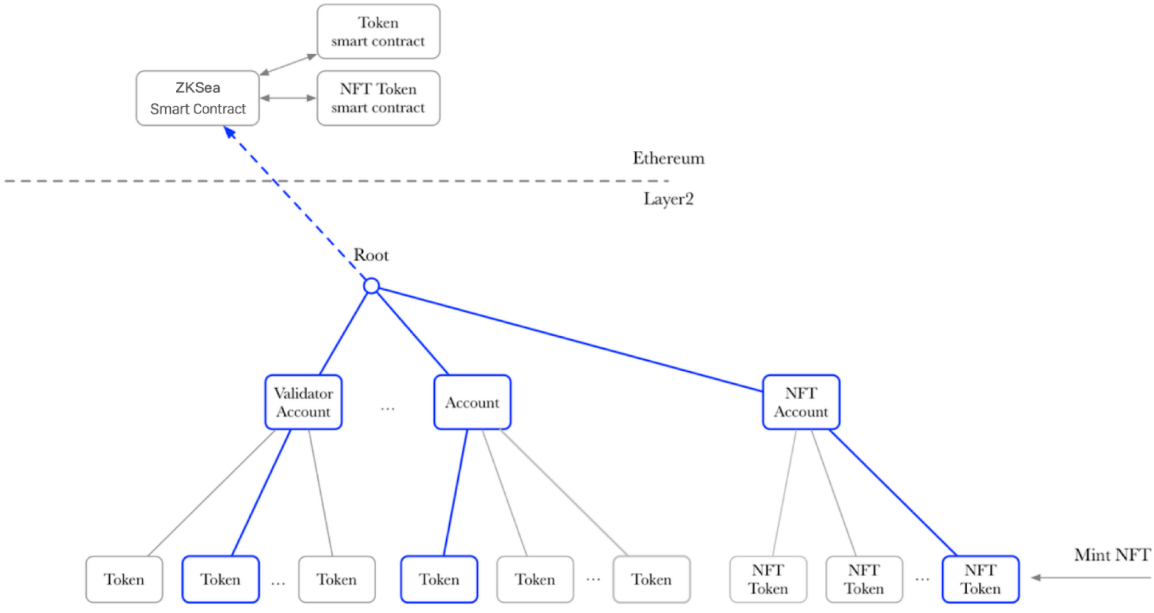

#### 4.2.3.2 Withdraw NFT

It is opposite to the procedures of NFT deposits. Details are shown as follows:



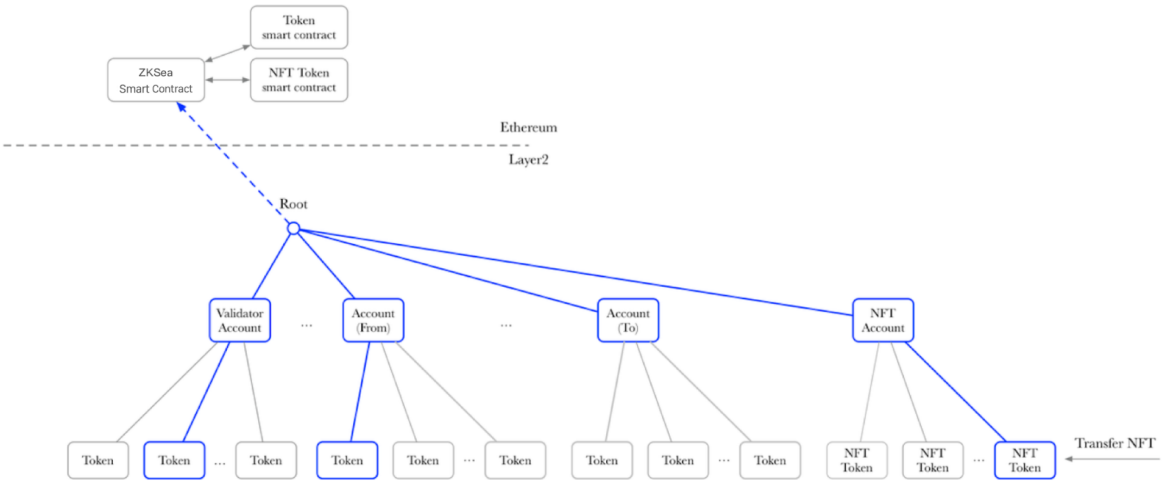

#### 4.2.3.3 Mint NFT

If the NFT can be directly created on layer-2, the steps are similar to that of NFT deposits. Details are shown as follows:



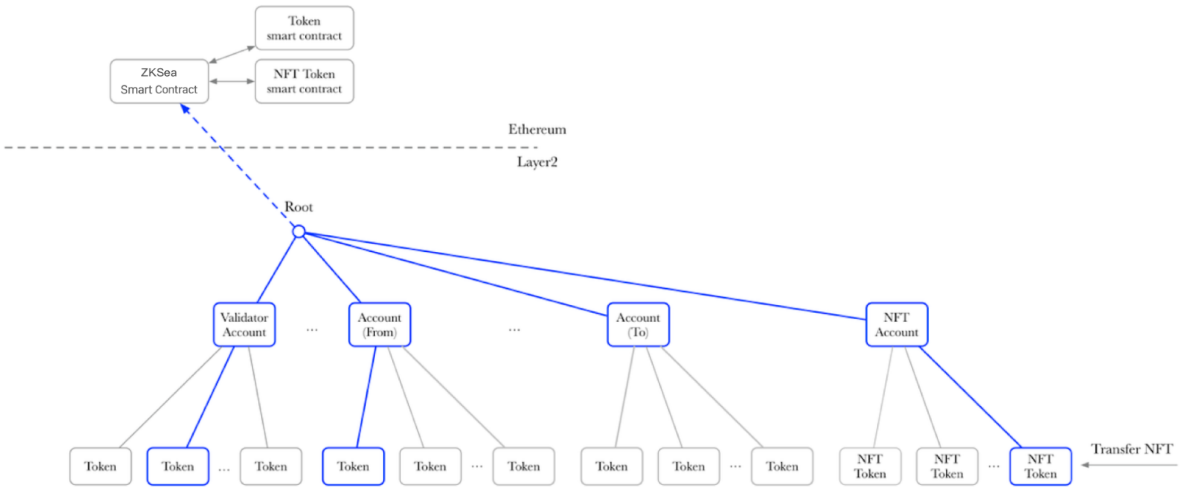

#### 4.2.3.4 Transfer NFT

Transfer the ownership of the NFT to the current account on layer-2. Details are shown as follows:



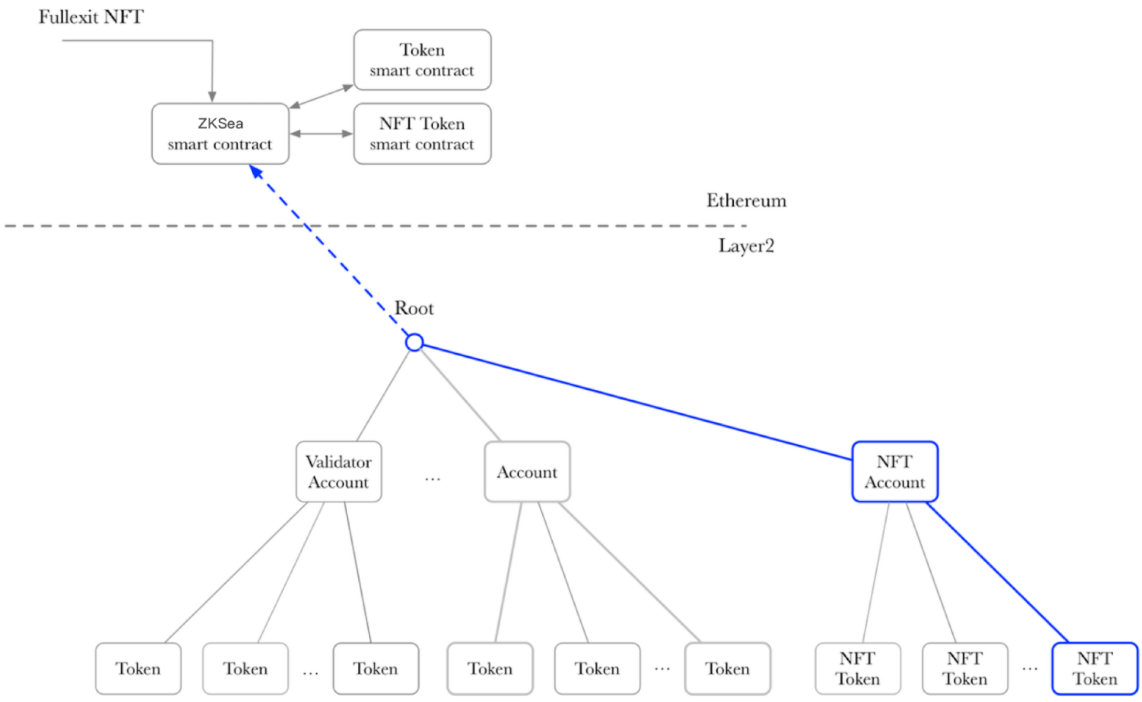

#### 4.2.3.5 Transfer To New NFT

Transfer the ownership of the NFT to the new accounts on layer-2. Details are shown as follows:



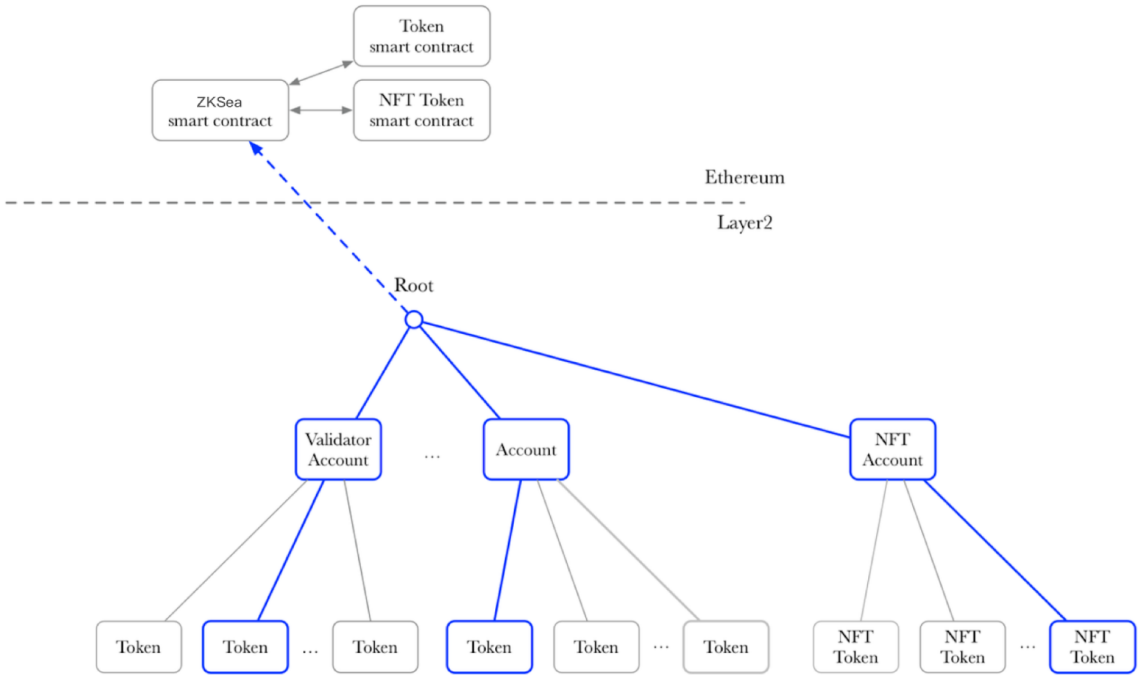

#### 4.2.3.6 Full Exit NFT

After initiating the withdrawal transaction from Layer-1, the procedures are shown as follows:



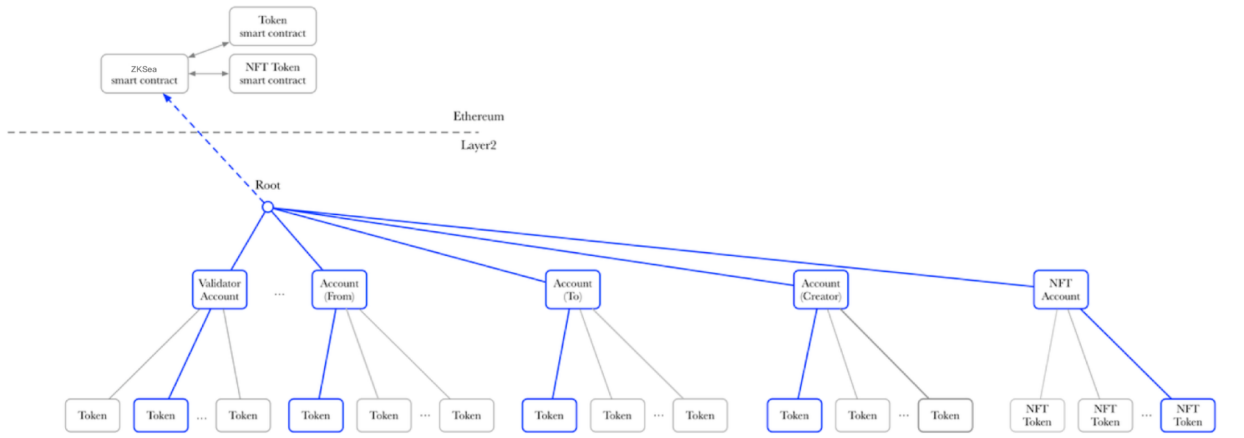

#### 4.2.3.7 Approve NFT

Each Layer-2 account can authorize its own NFT, that is to authorize one Layer-2 account to purchase the amount of this NFT. The approved_token can only be a fee token or a user token. Details are shown as follows:



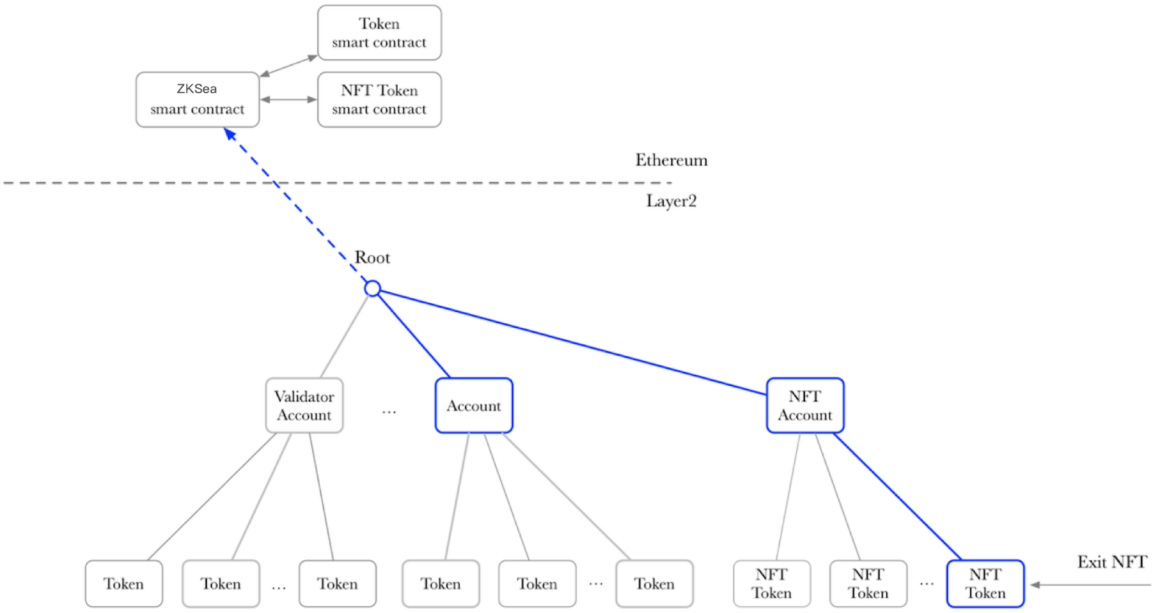

#### 4.2.3.8 Exchange NFT

Except for exchange NFT between “from” and “to”, Exchange NFT also needs to transfer part of the cost of the traded token to the creator. Details are shown as follows:




#### 4.2.3.9 Exit NFT

When entered into the Exodus mode, users can initiate a request of Exit NFT on Layer-1, to extract a certain NFT to Layer-1. Details are shown as follows:




# 5. Summary and Outlook

The ZKSquare protocol, using ZK-Rollups technology, has provided a complete solution including DEX, Payment, and NFT on layer-2 and it is a set of full-featured decentralized protocols of Layer-2 with infinite scalability and high TPS. Furthermore, the gas fee of all token transactions on layer-2 is as low as one-tenth of that of the mainnet, and it supports real-time transactions, with which users can experience rapid transactions without waiting for block confirmation. Such functions greatly remove the barriers for users to use blockchain applications. Meanwhile, the security on layer-2 is the same as the master net Layer-1, and thus the users' assets are kept in their wallets at all times, and they can also withdraw their assets to Layer-1 at any time.

The ZKSquare protocol is supported and developed by L2 Labs. In the future, L2 Labs will continue to drive the iteration and update of the Layer-2 protocol layer to support more transaction types and protocol types, and at the same time to further improve processing performance and TPS. We will open the source of the complete underlying protocol to the community, and create a complete Layer-2 DeFi and NFT ecosystem with the blockchain application developers. As well, on the basis of the ecological development, we will deploy to other public chains (such as BSC and SOLANA) besides Ethereum, and make it accessible to transfer funds on Layer 2 between different chains, so that users can quickly complete the cross-chain transactions with a low cost.

Since 2021, the users and market size of the DEFI and NFT have surged, however, when compared with the traditional financial or art collectibles market, it's still a blue ocean. L2 Labs is devoted to creating a Layer-2 protocol standard to provide users with a better experience,

making Layer-1 the base of clearing and settlement, and Layer-2 the bridge and link connecting blockchain applications and Layer-3. We will focus on the development and technological evolution of the blockchain application industry continuously, spread the best blockchain applications to more people, and then lead a paradigm shift in the blockchain industry.

We will open-source the Layer 2 infrastructure and formulate a Layer 2 ecological incentive plan to invite developers to access Layer 2 services for free, and thereby build a prosperous Layer 2 ecosystem together.

# References


1. Uniswap is a decentralized protocol for automated liquidity provision on Ethereum.
https://Uniswap.org/.
2. Be a DeFi Chef with Sushi.
https://docs.sushi.com/
3.OpenSea Developer Platform - The first and largest NFT marketplace.
https://docs.OpenSea.io/
4. Alex Gluchowski. Zk rollup: scaling with zero-knowledge proofs.
https://pandax-statics.oss-cn-shenzhen.aliyuncs.com/statics/1221233526992813.Pdf.
5. Uniswap v1.
https://Uniswap.org/docs/v1/.
6. Uniswap v2.
https://github.com/Uniswap/Uniswap-v2-core.
7. Ariel Gabizon, Zachary J. Williamson, and Oana Ciobotaru. Plonk: Permutations over lagrange-bases for oecumenical non-interactive arguments of knowledge. Cryptology ePrint Archive, Report 2019/953, 2019.
https://eprint.iacr.org/2019/953.
8. ZKSwap v1.
https://github.com/l2labs/zkswap-whitepaper/blob/master/zkswap_en.pdf
9. ZKSwap v2.
https://github.com/l2labs/zkswap-whitepaper/blob/master/zkswap_v2_en.pdf