ZKBox White Paper

Content

1. Introduction

Since 2019, decentralized finance (DeFi) has risen rapidly. Based on Ethereum and major public chains, blockchain developers have created a series of applications such as exchanges, mortgage lending, stablecoins, insurance, oracles, and games. An increasingly complete decentralized financial ecosystem has been formed. The vigorous development of blockchain technology and applications attracts more and more new users. The global liquidity easing policy has brought a steady stream of abundant funds for DeFi. According to defillama data, the total value locked in the DeFi field has exceeded 180 billion U.S. dollars. Among them, the total value locked on Ethereum has been at the top, and public chains or side chains such as BSC, Terra, Solana, Fantom, and Maitc have shared most of the remaining market shares.

If DeFi has brought initial users and funds to the public chain, then GameFi and NFT have brought more playability and collection value to the public chain, which can also attract a large amount of out-of-circle traffic and funds. Due to the performance limitations of the current blockchain, it is still difficult to make a big difference in games. Not surprisingly, NFT has inherited the popular market of DeFi. More and more influential people from all walks of life are paying attention to, buying and issuing NFTs. Most issuers and consumers have chosen the more decentralized and ecologically mature chain - Ethereum. OpenSea, the world's largest NFT trading platform, had a transaction valued at $3.4 billion on Ethereum in August 2021, an increase of more than 10 times over July. The most popular among them is the CryptoPunks series, which has generated about 202,000 ETH transactions in the past month. Converted at the current price of ETH, the transaction value is nearly 800 million U.S. dollars. People's high attention and enthusiasm for NFT can be seen.

In this context, more and more artists or projects have begun to create and issue NFTs. Faced with a larger user scale and the size of the NFT market, congestion on Ethereum has begun, and gas fees have become an expense that users cannot ignore. Excluding the price of the artwork itself and the commission paid to the trading platform, users often need to pay a gas fee of up to hundreds of dollars for a transaction, which is unacceptable for ordinary users and some artists who are not well-known. Even it may "dissuade" many people outside the circle who are interested and discourage more writers in the field of traditional art or consumers from NFT. Second, subject to the limitations of the Ethereum mainnet TPS, congestion will occur when the number of users surges, resulting in long time in onchain transactions and confirmation. Moreover, if the transaction fails due to being preempted after a long wait, people may lose their patience and heart. Therefore, we can see that many authors and projects even use the method of free transfer of the copyright of their works to attract users to pay gas fees to cast NFTs. They do not seek profit, but only hope that their works can be cast into NFTs for circulation on the chain. It is very detrimental to promote the ecology of artists.

According to this, after months of exploration and research, the L2 Labs team, which has been cultivating zero-knowledge proof for many years, creatively launched the ZKBox protocol. Based on ZK-Rollups technology, the NFT minting, circulation, and transaction processes on the Ethereum mainnet have been shifted to Layer 2. Multiple transactions can be aggregated and packaged onchain, and the state consistency of the Ethereum mainnet Layer 1 and Layer 2 are guaranteed through continuously generated zero-knowledge proofs. Also, it can achieve real-time NFT minting and transactions with zero Gas fee,

get rid of the limitations of Ethereum TPS and block confirmation time, and make users have the silky experience of a centralized platform of the NFT minting and transaction process and control the security of their own funds in real-time, ensuring the same degree of security as the Ethereum mainnet. We believe that the launch of the ZKBox protocol not only can greatly improve users' experience in the NFT minting and transaction process but can return the pricing power of NFT works to the artists and the market, without being subject to high gas fees any longer. We will also open ZKBox to any NFT platform.

At present, most of the development work has been completed, and we will officially launch the ZKBox protocol and development documents in October 2021. The first version of the ZKBox protocol will have the following features:

1) minting NFT with zero gas fee on Layer 2 network;
2) NFT's zero gas fee transaction and transfer functions on Layer 2 network, and theoretical TPS up to thousands;
3) Free deposit and withdrawal of NFT between Layer 1 and Layer 2 of the ETH mainnet.

In the future, the ZKBox protocol will further improve the performance of the Layer 2 network and support more contract types of NFTs. The L2 Labs team will also promote the "Layer 2 for all" multi-chain ecological strategy, and consider deployment based on the development of the NFT industry on the BSC, Solana and other chains, contributing to the ecological prosperity of each public chain.

2. Background and Technologies

2.1. Background

NFT, or Non-Fungible Token, is irreplaceable and unique. It means that it can digitize some unique artworks or assets in reality, such as a piece of Beethoven's music, a painting by Van Gogh, etc.

NFT, like mainstream crypto assets such as Bitcoin (BTC) and Ethereum (ETH), will be recorded on the blockchain, open to everyone, and cannot be tampered with. The difference between NFT and mainstream blockchains is that all NFTs are unique and indivisible. When you purchase an NFT, it means that you have obtained its exclusive rights and the right to use actual assets. For example, if you purchase an NFT weapon in the game, its display rights and use rights will belong to you unconditionally, unless you voluntarily transfer it; if you purchase an NFT artwork, you will get its actual use rights and copyrights.

NFT is the only indivisible asset in the digital world, which can be minted, traded and used to anchor some physical commodities in the real world, and also can digitize assets in different fields. With the development of blockchain technology and the emergence of more NFT platforms and applications, more and more artists, celebrities and institutions have entered the NFT field. The current mainstream types of NFT include artworks, music, virtual world assets, game cards, collectibles, domain names, etc., which have extended to all aspects of life.

2.2. Technologies

2.2.1 NFT Protocol

Essentially, an NFT is a technical protocol standard with blockchain as the bottom layer in the process of asset digitization. Ethereum developers openly solicit opinions, hoping to define a unified communication interface and establish a set of standards that can be followed to make Ethereum developers write smart contracts more fluidly, so a series of general protocols called ERC (Ethereum Request for Comments) was born. Among the protocols that are widely used are:

(1) ERC-721 - The metadata structure of NFTs on Ethereum. ERC-721 is the first standard that represents non-fungible digital assets proposed by Dieter Shirley in September 2017, and it is also the most commonly used form of token in the NFT field. ERC-721 defines the minimum interface that a smart contract must implement to allow the management, ownership and trading of unique tokens. Under the ERC-721 standard, assets can be converted into the only and unique 256-bit tokens. And such tokens can be tracked through smart contracts on the blockchain to create digital assets.

(2) ERC-1155 - The Enjin team created the ERC-1155 standard protocol in June 2018, using a new way to define tokens. Items will be stored in a central smart contract and occupy very little space used to distinguish each other only. The ERC-1155 protocol can send multiple items in one transaction, which greatly improves the efficiency and convenience of transfers. On the other hand, it also reduces gas fees and network resource consumption.

(3) ERC-998 - Composable NFT. It was originally proposed by Matt Lockyer. The ERC-998 protocol can package different types of tokens (ERC-721 type tokens and ERC-20 type tokens) to achieve the ability of combined transfer.

(4) ERC-420 - It was originally proposed by PepeDapp, which can be used as a digital transaction card standard.

The current NFT standard protocol with the highest market share is ERC-721, followed by ERC-1155. Developers can easily generate a batch of similar NFT assets according to the protocol standard. With the expansion of the NFT market and the development of blockchain technology, we believe that there will be more NFT standard protocols in the future to meet the different needs of users. The following introduces and analyzes the mainstream ERC-721 and ERC-1155 standard protocols.

2.2.2 ERC-721 standard protocol

https://eips.ethereum.org/EIPS/eip-721
It is mainly composed of three interfaces:
ERC-721 is the main interface:
- balanceOf - query the number of NFTs under an address
- ownerOf - query the owner of a certain NFT
- transferFrom series of functions-NFT transfer
- approve approve series of functions-authorization and query of NFT

```
JavaScript
interface ERC721 /* is ERC165 */ {

    event Transfer(address indexed _from, address indexed _to, uint256 indexed
_tokenId);
    event Approval(address indexed _owner, address indexed _approved, uint256
indexed _tokenId);
    event ApprovalForAll(address indexed _owner, address indexed _operator, bool
_approved);

    function balanceOf(address _owner) external view returns (uint256);
    function ownerOf(uint256 _tokenId) external view returns (address);
    function safeTransferFrom(address _from, address _to, uint256 _tokenId, bytes data)
external payable;
    function safeTransferFrom(address _from, address _to, uint256 _tokenId) external
payable;
    function transferFrom(address _from, address _to, uint256 _tokenId) external
payable;

    function approve(address _approved, uint256 _tokenId) external payable;
    function setApprovalForAll(address _operator, bool _approved) external;
```

```
        function getApproved(uint256 _tokenId) external view returns (address);
        function isApprovedForAll(address _owner, address _operator) external view returns
(bool);
}
```

Create NFT with ERC-721Metadata interface:

- name - name
- symbol - Token name
- tokenURI - URI information corresponding to a certain NFT

```
TypeScript
interface ERC721Metadata /* is ERC721 */ {
        function name() external view returns (string _name);
        function symbol() external view returns (string _symbol);
        function tokenURI(uint256 _tokenId) external view returns (string);
}
```

The ERC-721Enumerable interface realizes the query function of NFT:

```
JavaScript
interface ERC721Enumerable /* is ERC721 */ {
        function totalSupply() external view returns (uint256);
        function tokenByIndex(uint256 _index) external view returns (uint256);
        function tokenOfOwnerByIndex(address _owner, uint256 _index) external view
returns (uint256);
}
```

https://github.com/0xcert/ethereum-erc721

2.2.3 ERC-1155 standard protocol

For details, please refer to:
https://github.com/ethereum/EIPs/issues/1155

2.2.4 ERC-721 VS ERC-1155

2.2.4.1 Fungible and Non-fungible

ERC-721: Non-fungible tokens only.
ERC-1155: Fungible and non-fungible tokens are all allowed, and new tokens like semi-fungible tokens are also allowed. For example, fungible tokens can be "transformed" into non-fungible tokens and vice versa.

2.2.4.2 Batch Transfer

ERC-721: Only one token per transfer is supported.
ERC-1155: Supports batch transfer of multiple token IDs in a single transaction.

2.2.4.3 Localization

ERC-721: Only one language is supported.
ERC-1155: Support the language localization of all metadata (such as token name, description, and even token image) so that all tokens are in common use.

2.2.4.4 Legacy metadata

ERC-721: Legacy metadata like "symbol" and "name" are retained, but this is unnecessary for many modern tokens.
ERC-1155: Save all metadata to URI (short for "Uniform Resource Identifier") on the web or IPFS.

2.2.4.5 ID replacement

ERC-721: Since only static metadata is supported, each token ID must be stored and managed by a smart contract with its metadata URI.
ERC-1155: The contract can point to countless token URIs without storing any additional data on the chain. It can even be used to point to a web service that dynamically generates token JSON for each token in the database.

2.2.4.6 Enrich Event Log

ERC-721: Can issue transfer and approval events.
ERC-1155: Standard events that can send coins, destroy, transmit, approve and change metadata, which can benefit the ecosystem, such as in-depth analysis of tokens and token browsers.

3 Scaling

3.1 Background

As the most active development platform in the blockchain world, the Ethereum network, with daily congestion and higher and higher handling fees, makes the applications and users in the ecosystem miserable. Coupled with the explosion of the NFT market, there are more and more congested transactions on Ethereum. If this kind of bad experience cannot be improved, it will have a negative impact on the development of Ethereum.

Therefore, in recent years, more and more blockchain researchers and developers have devoted themselves to the research of the underlying technology and tried various technical means to improve the state of the entire network. There are technical solutions for Layer 1, such as the sharding technology of ETH 2.0, which improves the efficiency of the network by modifying or optimizing the consensus network of the blockchain, thereby speeding up the block confirmation time and achieving the purpose of the fast transaction on the chain; there are also technical solutions for Layer 2. Under the premise of keeping Layer 1's functions simple, powerful and stable, some calculations and operations originally on Layer 1 are put on the chain to finish, and then ensure the accuracy of these off-chain operations through cryptography technology.

But from a long-term point of view, the scaling technology solution based on Layer 2 will be more suitable for the healthy development of blockchain.

Since the blockchain infrastructure is relatively clear, stable and easy to maintain, imposing complex logic based on this may make Layer 1 more and more fragile. Therefore, the development direction of the blockchain structure should be Layer 1 to remain unchanged as much 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, and other complex logic and innovative applications should be placed on Layer 2. Layer 1 and Layer 2 complement each other.

Researchers have gradually discovered this. Therefore, the expansion technology solutions based on Layer 2 are emerging one after another. However, the ideal is wonderful, but the reality is very skinny. When the theory needs to be practiced, the developers discovered that there are too many places to weigh the pros and cons in order to achieve expectations. For different application scenarios, they may have to make different compromises.

3.2 ZK-Rollups

So far, among the Layer 2 expansion plans, the most discussed are ZK-Rollups, Optimistic Rollup, Validium and Plasma.

ZK-Rollups: It was proposed by the researchers of Ethereum, the feature of which is that all calculation processes are completed off-chain and stored on-chain, and the plaintext data involved in the calculation is sent to the on-chain contract in the form of calldata, reducing storage costs; at the same time, the

correctness of off-chain calculations is guaranteed by zero-knowledge proof algorithm. It can also be seen that this solution can not only greatly increase the TPS, but also reduce the cost of a single transaction.

Optimistic Rollup: It is divided into Optimistic Rollup (ORU) and Arbitrum Rollup (ARU). Both use a challenge mechanism to ensure safety. The difference between them is that the challenge mechanism of ORU is to challenge a transaction, that is, the EVM must completely execute a challenged transaction, while ARU treats the execution process of the transaction as an orderly order through the subdivision, and the problematic order is found to be challenged through multiple rounds of interaction, making the verification cost very low. **But compared to ZK-Rollups, Optimistic Rollup's security assumptions are weaker.**

Validium: This plan was proposed by StarkWare and was approved by God V, so it was named. The characteristic is that the calculation process is completed off-chain, the correctness of the calculation is guaranteed by the zero-knowledge proof algorithm, the verification is completed on the chain and the final world state is stored. One more thing to note is that in order to obtain better scalability, this solution also stores transaction data off-chain, and at the same time, a credible "data availability" committee provides proof of data availability. Compared with the previous two schemes, this scheme loses a certain amount of data availability, but it does provide better data scalability. Therefore, in actual application scenarios, this scheme may be more favored.

Plasma: It was proposed by God V. Compared to the other three proposals, this proposal was proposed the earliest. The features of this solution are remarkable that it is calculated off-chain, stored on-chain, and transaction data is also stored off-chain, which is very simple. Users can initiate wrong proofs to prove the executor's evil behavior, thereby obtaining rewards and punishing the evil executors.

There is no doubt that only ZK-Rollups can bring the same degree of security to our system as Layer 1, which is why we chose it.

3.3 Aggregative proof

The ZK-Rollups solution is based on a zero-knowledge proof algorithm to ensure that the changes in the world state caused by all transactions in a block are correct. Multiple transactions are processed at one time to achieve the first improvement in system performance and bring higher TPS. However, due to the limitation of the circuit scale, the improvement effect brought by this solution did not meet expectations, and it was not enough to support the current amount of Layer 2. Therefore, an additional technical protocol was needed to improve the overall performance, which is Aggregative Proof.

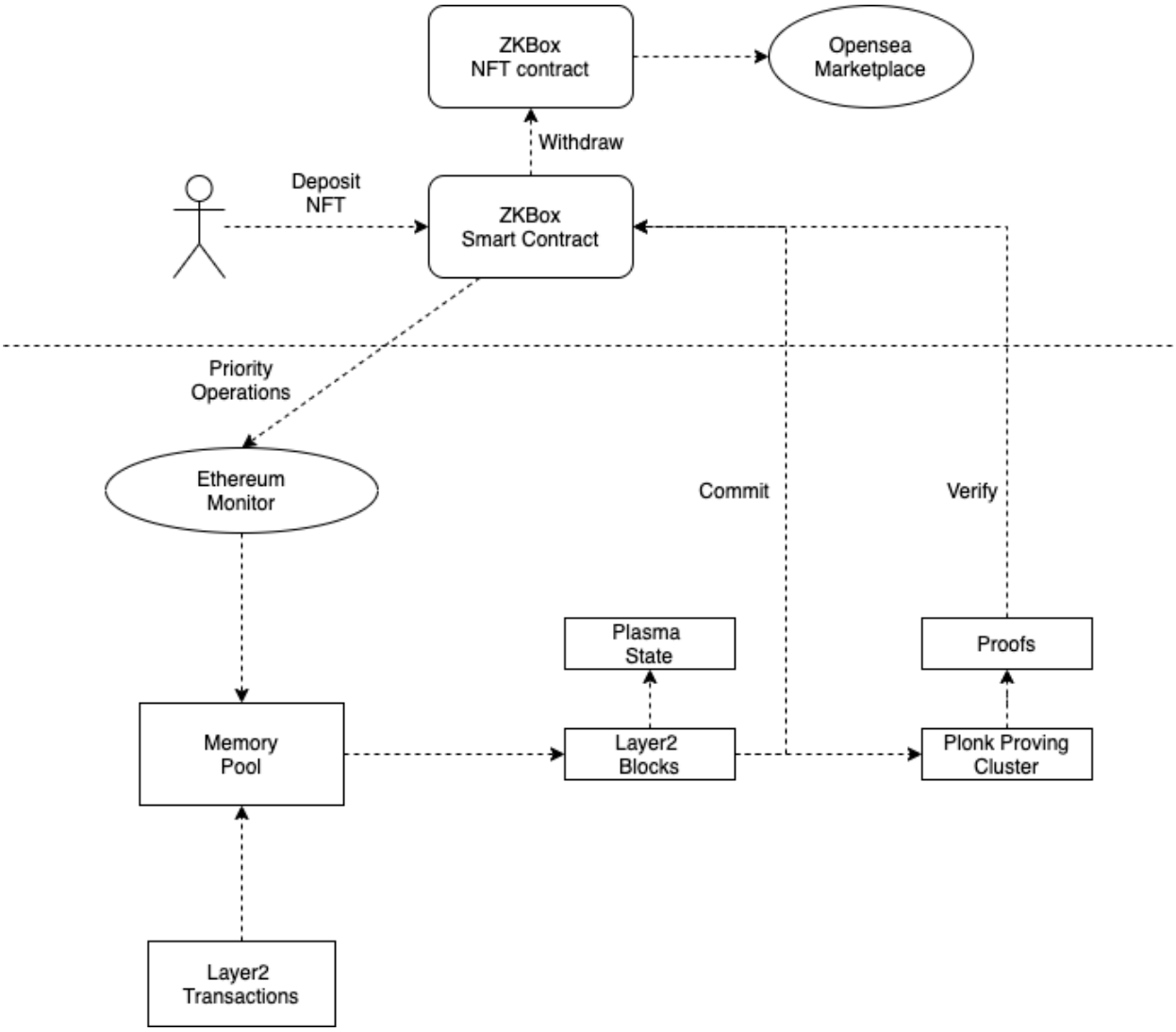
The logic of aggregate proof is actually very simple. As we all know, in the basic Layer 2 expansion plan, a block corresponds to a proof of validity, and the validity of the proof of validity is verified by the contract on the chain. At present, the average block generation speed of Ethereum is 15s per block. If the validity of multiple blocks can be verified on the chain at a time, the cost amortized on each transaction will be greatly reduced. The so-called aggregation proof scheme is that, now with a proof for each block, prove the multiple proofs generated within a period of time or a fixed number of blocks are valid. (Think of the verification process as a kind of circuit). In this way, only one time of verification is needed on the

chain to verify the validity of multiple block proofs. The schematic diagram of the aggregate proof is shown in the figure below:

Data	Type	Size	Comments
tx_op	uint8	1	16
from	AccountID	4	the account id of from
nft_id	uint64	8	the global NFT id
creator	AccountID	4	the account id of creator，0 - NFT from 3rd party
seq_id	uint32	4	seq id，0 - NFT from 3rd party
uri	bits	32	0 - NFT from 3rd party
to_eth_addr	Address	20	the Ethereum address of to
fee_token_id	uint8	1	
fee	FEE_EXPONENT_BIT_WIDTH + FEE_MANTISSA_BIT_WIDTH	2	

4. NFT protocol of ZKBox--Layer 2

4.1 ZKBox system framework



4.2 NFT Model Design

Information related to NFT expansion in the account information:

- Seq ID - When each Layer 2 account issues an NFT, the Seq ID increases by 1.

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

- Global Token ID-NFT ID global number, 64bit
- Creator-NFT's creation account ID, 32bit

• NFT Seq ID-the NFT serial number of the Layer 2 account, 32bit
• URI information-CID information of IPFS, CID V0, 32 bytes-256bit
• Owner Account ID-Owner account number, 32bit
• Approved Account ID-Authorized account number, 32bit (if it is 0, there is no limit to purchase accounts)
• Approved Token ID-Authorized Token ID, 16bit
• Approved Token Amount-NFT offer price, 128bit

Layer 2 account must specify NFT Seq ID when creating NFT (Mint NFT). Seq ID is equal to account.SeqID + 1. Global Token ID, Layer 2 can be selected randomly, as long as it is guaranteed to create a new account on an empty account. Approved related information specifies information related to "purchase", such as who can purchase at what price.

For all NFTs created by a Layer 2 account, related information is stored on IPFS, and each NFT has unique URI information.

The NFT in the Layer 2 account has two numbers:
1. Global NFT ID;
2. Creator + Seq ID.

Global NFT ID is a globally unique identifier.

Account starting from number 2^27 are reserved for storing NFT information:

4.2.1 Account Model

A total of 2^28 accounts are supported. Among them, 2^27 ordinary accounts are supported, and account 0 is the Validator account (fee account). The other 2^27 accounts are reserved for NFT function.

4.2.2 Token Model

Three types of tokens are supported, divided into two types:
• AMM Token: Fee Token, User Token and LP Token (2^16 in total)
• NFT: Any leaf on the reserved Account is an NFT. There is no difference between them.

Name	Type	Number	Comments
Fee Token	-	0~31	0 - ETH（reserved），32 in total
User Token	-	32~16383	16352
LP Token	-	16384~65535	49152
NFT	-	-	2^16*2^27，support 2^43 NFT in total

4.2.3 Global Token ID

Global Token ID is the unique identification of each NFT between Layer 1 and Layer 2. Any NFT that has existed in Layer 2 will be given a globally unique Global Token ID. A certain Layer 2 NFT, from Layer 2 "withdraw" to Layer 1, still maintains the corresponding relationship between the unique label of Layer 1 and the Global Token ID in Layer 1. If the NFT deposits to Layer 2 again, Layer 2 will continue to use the previous Global Token ID, and no new ID will be generated. All NFTs generated on Layer 2 have an exclusive Global Token ID number. The relationship between Global Token ID and Account ID/Balance ID is as follows:

```
Apache
global_token_id = (account_id - 2^27) << 16 + balance_id + 1
```

4.2.4 Creator/Seq ID

Creator/Seq ID refers to an account that creates an NFT on Layer 2. It should be pointed out that a certain NFT Creator is only valid for NFTs created on layer 2. The third-party NFTs deposited from Layer 1 to Layer 2 have lost the creator information. These NFTs do not have Creator and Seq ID in Layer 2. In other words, if a third-party NFT deposits from Layer 1 to Layer 2, the Creator is set to 0. Because in Layer 2, the Validator (account ID is 0) does not participate in any NFT transactions, so setting the Creator to 0 means that there is no Creator. In particular, the NFT belonging to the platform deposited from Layer 1 to Layer 2 must maintain the original creator and seq ID. As shown in the following table, only when the third-party NFT deposits for the first time, the NFT has no relevant information about the deposit/withdraw operation between Layer 1 and Layer 2. In other cases, the basic information of the NFT remains unchanged, whether on Layer 1 or Layer 2.

Type	Is 3rd Party?	Exist on L2 before?	Info	Comments
deposit	Y	Y	☑	
deposit	Y	N	☒	
deposit	N	Y	☑	
deposit	N	N	☑	
withdraw	Y	Y	☑	
withdraw	Y	N	-	
withdraw	N	Y	☑	
withdraw	N	N	-	

4.2.5 Information

All NFTs participating in the issuance on Layer 2 will use the same BaseURI. The URI of the specific token is distinguished by BaseURI + tokenID. Subsequent versions may be upgraded to a different BaseURI for each item.
The NFT issued by other third parties on Layer 1 uses the original URI and remains unchanged.

4.2.6 Balance Extension

Account is divided into two types, one is Token Account (including Pair Account), and the other is NFT Account. The balance of Token Account is the balance corresponding to a certain Token, 128 bits. The balance of the NFT Account is the "truncated" result of the hash corresponding to the NFT info, 128 bits.

4.2.7 Approved Info

Approved Info needs to express three states: 1/ No Approved Info 2/ Anyone can purchase 3/ Designated talents can purchase.

Name	Number	Meaning	Comments
Approved Account ID	0	Anyone can purchase	
	owner	Cannot purchase	
Approved Token ID	Valid token ID		0 - ETH
Approved Token Amount	Any valid amount		Including 0

4.3 NFT Operational Design

The NFT issued on layer 2 is managed by a unified number (NFT ID). All NFT operations on Layer 2 are charged.

4.3.1 Deposit NFT

By initiating a Deposit request from Layer 1, the NFT of Layer 1 can be mapped to Layer 2. For Layer 1 NFT, the ZKBox smart contract will mobilize the NFT smart contract to create the corresponding NFT. All NFTs issued in Layer 2 are managed by the NFT smart contract.

Note: The NFT ID of the third-party NFT from Layer 1 Deposit can be "assumed" that it is not a random number, similar to a sequential value starting from 1, and less than the power of 2^252. View popular NFTs: https://etherscan.io/tokens-nft

There are two situations for Deposit NFT: 1/ Third-party NFT deposit 2/ Once issued on Layer 2, and withdraw to Layer 1. In the case of a third-party NFT, only the corresponding Global NFT ID (nft_id) needs to be created in Layer 2. The specific information of this NFT is recorded on layer 2. In order to correspond to the deposit processing sequence of Layer 1, Layer 2 and Layer 1 are synchronized through priority_op_id.

For the second case, the specific information of NFT needs to be synchronized between Layer 1 / Layer 2 (including Creator/Seq_id/URI/Owner).

4.3.1.1 (Onchain Op) pubdata

Data	Type	Size	Comments
tx_op	uint8	1	12
nft_id	uint64	8	Global Token ID
creator	AccountID	4	the account id of creator，0 - NFT from 3rd party
seq_id	uint32	4	seq id，for 3rd party, one global ID is generated on L1
uri	bits	32	0 - NFT from 3rd party
from	Address	20	the owner of this NFT
from_account_id	Account ID	4	account id of from in L2

4.3.1.2 Priority Operation

Data	Type	Size	Comments
creator	AccountID	4	the account id of creator
seq_id	uint32	4	seq id
uri	bits	32	
from	Address	20	the owner of this NFT

4.3.1.3 Rollup Operation

Data	Type	Comments
op	DepositNFTPriorityOp	12
nft_id	uint64	Global Token ID
from_account_id	Account ID	account id of from in L2

4.3.2 Withdraw NFT

4.3.2.1 pubdata

Data	Type	Size	Comments
tx_op	uint8	1	16
from	AccountID	4	the account id of from
nft_id	uint64	8	the global NFT id
creator	AccountID	4	the account id of creator，0 - NFT from 3rd party
seq_id	uint32	4	seq id，0 - NFT from 3rd party
uri	bits	32	0 - NFT from 3rd party
to_eth_addr	Address	20	the ethereum address of to
fee_token_id	uint8	1	
fee	FEE_EXPONENT_BIT_WIDTH + FEE_MANTISSA_BIT_WIDTH	2	

4.3.3 Mint NFT

NFT can be created directly on Layer 2, and the change of the world state is similar to Deposit NFT.

4.3.3.1 pubdata

Data	Type	Size	Comments
tx_op	uint8	1	13
seq_id	uint32	4	seq id
nft_id	uint64	8	global nft id
from	Account ID	4	the account that issued this NFT
uri	bits	32	
fee_token_id	uint8	1	
fee	FEE_EXPONENT_BIT_WIDTH + FEE_MANTISSA_BIT_WIDTH	2	

4.3.4 Transfer NFT

Transfer NFT: Transfer of NFT ownership.

4.3.4.1 pubdata

Data	Type	Size	Comments
tx_op	uint8	1	14
from	AccountID	4	the account id of from
to	AccountID	4	the account id of to
nft_id	uint64	8	global nft id
fee_token_id	uint8	1	
fee	FEE_EXPONENT_BIT_WIDTH + FEE_MANTISSA_BIT_WIDTH	2	

4.3.5 TransferToNew NFT

TransferToNew NFT: Transfer NFT to the new account.

4.3.5.1 pubdata

Data	Type	Size	Comments
tx_op	uint8	1	15
from	AccountID	4	the account id of from
to	AccountID	4	the account id of to
to_addr	Address	20	the ethereum address of to
nft_id	uint64	8	global nft id
fee_token_id	uint8	1	
fee	FEE_EXPONENT_BIT_WIDTH + FEE_MANTISSA_BIT_WIDTH	2	

4.3.6 FullExit NFT

Withdrawal transactions initiated on Layer 1.

4.3.6.1 pubdata

Data	Type	Size	Comments
tx_op	uint8	1	17
from	AccountID	4	the amount id of from
nft_id	uint64	8	the global NFT id
creator	AccountID	4	the account id of creator, 0 - NFT from 3rd party
seq_id	uint32	4	seq id
uri	bits	32	0 - NFT from 3rd party
from_eth_addr	Address	20	the ethereum address of from
success	uint8	1	success or failed? 1 - success, 0 - failed

4.3.7 approve NFT

Each Layer 2 account can authorize the NFT it owns and authorize a Layer 2 account to purchase the amount of the NFT. Approved_token can only be fee token or user token.

4.3.7.1 pubdata

Data	Type	Size	Comments
tx_op	uint8	1	18
from	AccountID	4	the amount id of from
to	AccountID	4	the account id of to
nft_id	uint64	8	the global NFT id
approved_token	uint16	2	the user token used to pay for this NFT
approved_token_amount	AMOUNT_EXPONENT_BIT_WIDTH + FEE_MANTISSA_BIT_WIDTH	5	the amount of user token the buyer need to pay for this NFT
fee_token_id	uint8	1	
fee	FEE_EXPONENT_BIT_WIDTH + FEE_MANTISSA_BIT_WIDTH	2	

4.3.8 Exchange NFT

In addition to exchanging NFT between from and to, Exchange NFT also needs to transfer part of the transaction token fee to the creator.

4.3.8.1 pubdata

Data	Type	Size	Comments
tx_op	uint8	1	19
from	AccountID	4	the account id of from
to	AccountID	4	the account id of to
creator	AccountID	4	the account id of creator
nft_id	uint64	8	the global NFT id
fee_token_id	uint8	1	
fee	FEE_EXPONENT_BIT_WIDTH + FEE_MANTISSA_BIT_WIDTH	2	
creator_fee	FEE_EXPONENT_BIT_WIDTH + FEE_MANTISSA_BIT_WIDTH	2	Fees paid to creator

4.3.9 ExitNFT

After entering the Exdous mode, the user can initiate an ExitNFT request from Layer 1 to extract a certain NFT to Layer 1.

4.3.9.1 pubdata

Data	Type	Size	Comments
from	Address	20	the owner of this NFT
nft_id	uint64	8	Global Token ID
creator	AccountID	4	the account id of creator (optional)
seq_id	uint32	4	seq id**(optional)**
uri	bits	32	ipfs uri - CID V0

4.4 Contract design

4.4.1 Deposit

Layer 1 calls the depositNFT function to deposit into the NFT. There are two types of deposited NFTs: 1/third-party NFT 2/NFT once issued on Layer 2.

```
Lua
function depositNFT(IERC721 _token, uint256 _token_id, address _franklinAddr) external
```

The two types of NFT can be distinguished by _token.

After it being packaged in the depositNFT function, submit it to Layer 1 again through commitBlock, and update the NFT information through updateNFTToken.
The updateNFTToken function updates the mapping relationship of the NFT in the NFT Manager (the mapping between Layer 1 NFT ID and Layer 2 NFT ID).

```
Apache
function updateNFTToken(IERC721 _token, uint256 _token_id, uint256 _account_id,
uint256 _nft_id) external
```

If the deposit is an NFT issued on layer 2, call burn through the NFT Factory to destroy the corresponding NFT on Layer 1.

4.4.2 Withdraw NFT

The NFT of Layer 2 is extracted to Layer 1 through the withdrawNFT function. After each block has confirmed, ZKBox conract actively processes the corresponding withdraw request in the block.

```
Lua
function withdrawNFT(uint256 _nft_token_id, address _addr) external
```

4.5 Limitations

- Layer 2 accounts are 2^27 in total and Layer 2 NFT accounts are 2^43 in total.
- Each Layer 2 account can only create one NFT at a time.
- NFT imported from the third party of Layer 1, has no creator.
- The token id of the NFT imported from the third party of Layer 1, is less than 2^252.
- Validator account does not participate in any NFT transactions.

5. Summary

The ZKBox protocol uses ZK-Rollups technology to implement a series of functions such as NFT minting, transaction, and transfer on Layer 2, which eliminates gas fees and block confirmation time. It has the characteristics of real-time transactions and allows users to withdraw NFTs to Layer 1 of the Ethereum mainnet at any time, which solves the problem of high gas fees on the Ethereum mainnet for art creators and NFT traders. ZKBox supports ultra-high TPS, which greatly reduces the threshold for ordinary users to participate in the NFT world.

The existing NFT minting and trading platforms can introduce the L2 Labs-backed ZKBox protocol to significantly improve the user experience through Layer 2 network. In the future, L2 Labs will continue to promote the iteration and upgrade of the ZKBox protocol, which will support more transaction methods, more NFT protocols, and further improve processing performance and TPS.

Since 2021, although the number, transaction volume and Google search index of NFTs have shown explosive growth, they are still a blue ocean compared with the traditional art collectibles market or the Internet game market. Art souvenirs and virtual assets in games are more about consensus value. Considering security and convenience, it is most appropriate to use non-fungible chain assets such as NFT as a carrier. Therefore, in the long run, we believe the NFT market still has huge room for imagination. L2 Labs is committed to creating a Layer 2 protocol standard with a better user experience, making Layer 1 the foundation of clearing and settlement, and Layer 2 as the bridge and entrance connecting blockchain applications and Layer 3. We will continue to pay close attention to the development of the NFT industry and technological evolution and lead the paradigm change of blockchain applications together.