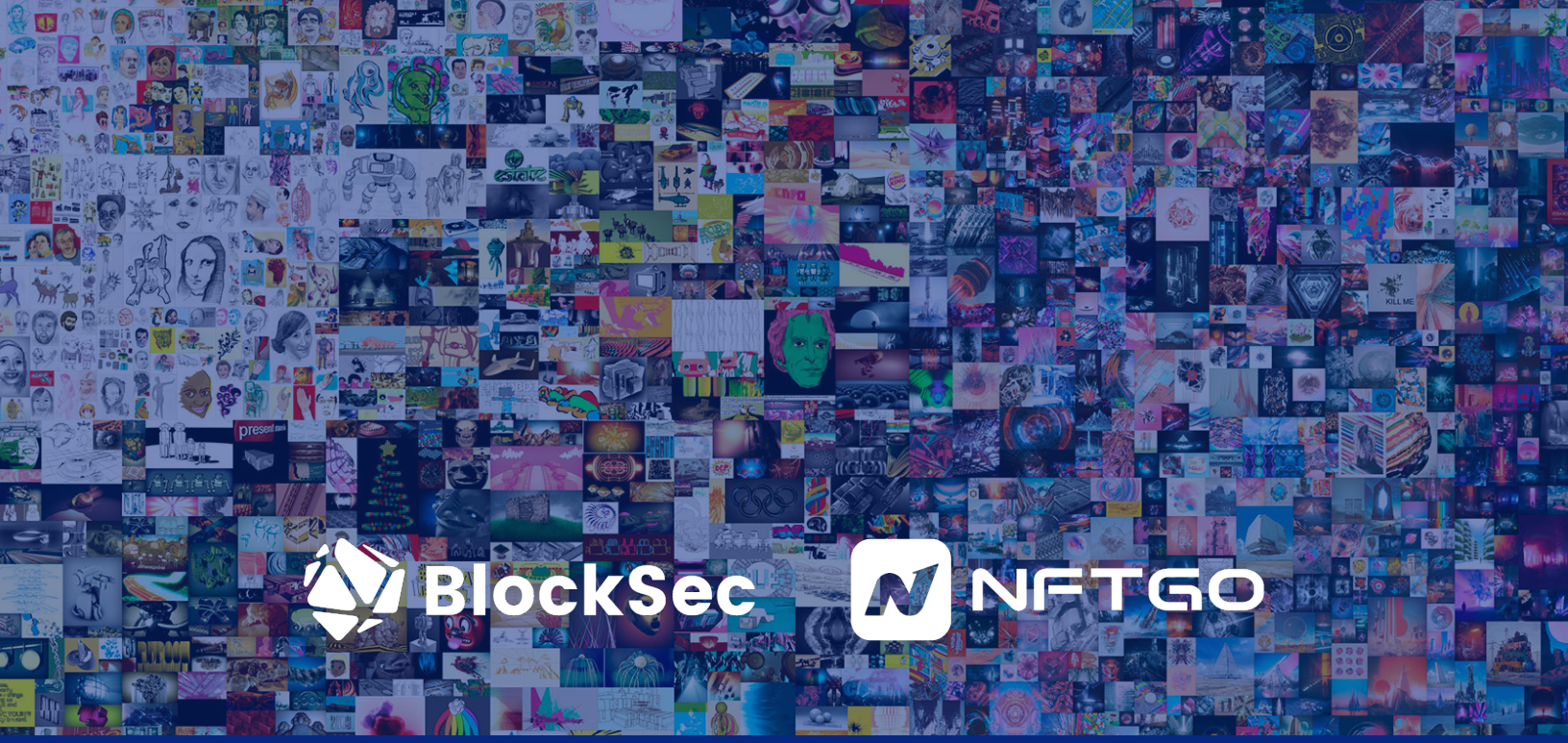

NFT Security Report 2022

Risk Detection, Quantifying and Solutions

NFT Security Report

Preface

Since last year, NFT and NFT markets have become popular decentralized applications. At the same time, many security incidents in the NFT ecosystem have been reported, which lead to significant financial loss. Though these reports demonstrated possible risks to users, they are disorderly information without systematic insights.

In this report, we show the result of a systematic study of the NFT ecosystem from the security perspective. Our study covers both the off-chain and on-chain security risks. Specifically, the off-chain security risk means the risk to NFT assets that are stored off the blockchain, and the on-chain security risk means the risk caused by the smart contracts and transactions that are on the blockchain.

Our study is mainly focused on Ethereum. The dataset consists of the smart contracts and related transactions from July 2015 to August 2022. It contains 119,900 NFT contracts, 83,100,000 NFT tokens issued from these contracts, and 25,900,000 NFT related transactions on markets.

Our analysis shows that:

1. Digital assets in around 19.0% (16.1K/84.8K) of the NFT projects are under the inaccessible risk. The potential financial loss reaches around 330.2K Ether (USD 515.1M)[1].

2. Nearly 55.4% (56.5K/102.0K) of the open-source NFT contracts have issues. Specifically, about 4.4K contracts have reentrancy and/or improper access control vulnerabilities. About 54.5K contracts have privilege functions that privilege users can operate normal users' assets without any permission.

3. The sleepmint attacks are carried out to deceive normal users into buying worthless NFT tokens. We found that 1,960 transactions involving 75 NFT contracts are sleepmint transactions.

4. About 61.8% (67.1K/108.5K) of the NFT projects are suffering from the holder pooling risk. These projects are over-centralized since one user (the biggest whale) holds more than 50% of tokens in the projects.

5. Wash trading is common in NFT marketplaces. The total wash trading volume reaches around 9.8M Ether (USD 15.2B), accounting for 43.0% of the total trading volume on OpenSea, LooksRare, and X2Y2. Most (87.5%) wash trading is on LooksRare.

[1] 1 Ether ≈ 1,550 USD on August 30, 2022

1. Introduction

1.1 NFT Ecosystem

According to Wikipedia, "**A non-fungible token (NFT)** is a record on the blockchain which is associated with a particular digital or physical asset." The ownership of an NFT is recorded on the blockchain and can be transferred by the owner, allowing NFTs to be sold and traded.

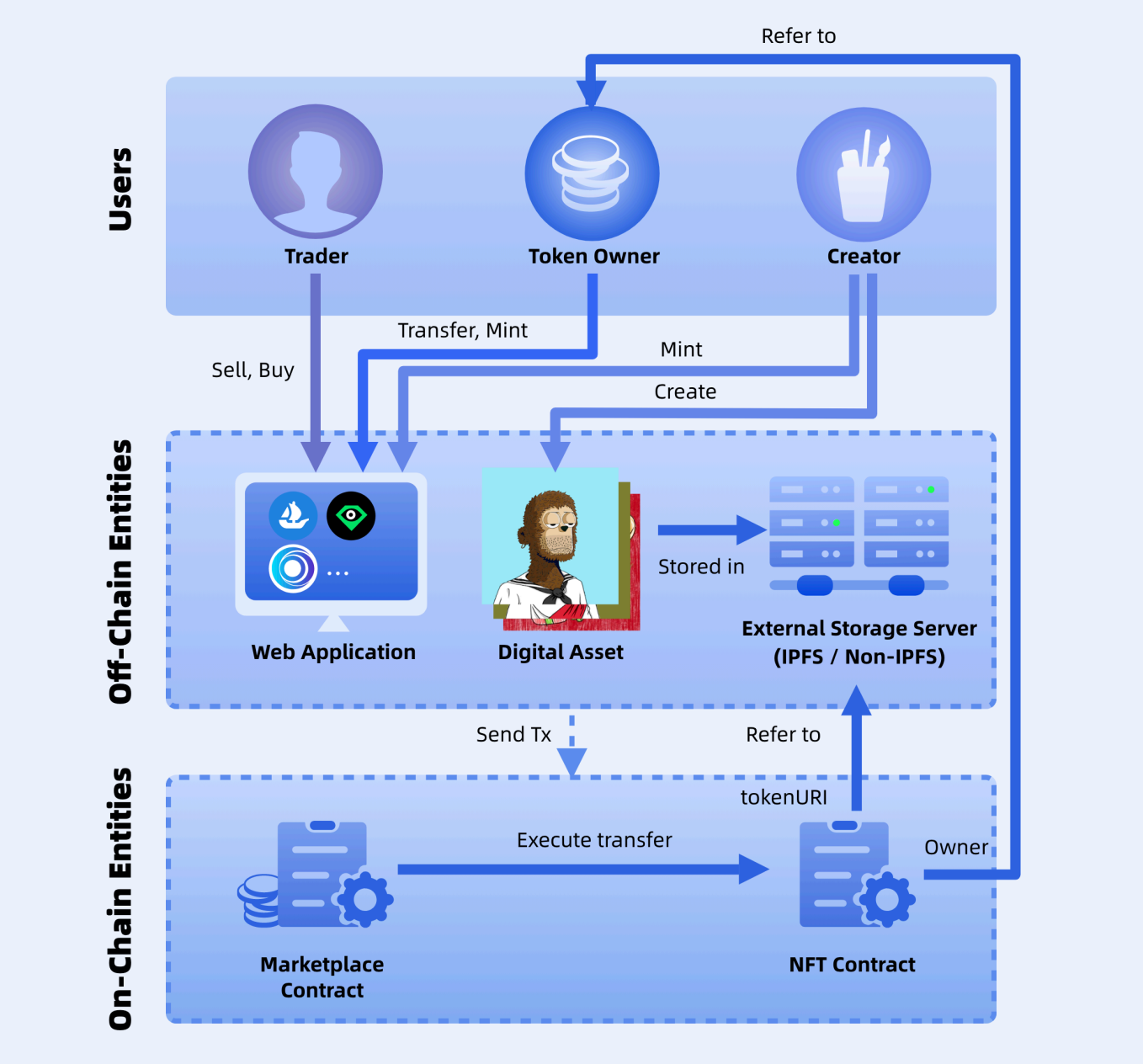

Fig. 1: The overview of the NFT ecosystem.

Fig. 1 presents an overview of the NFT ecosystem. There are three types of entities and two types of actions in the NFT ecosystem. The entities are users, off-chain entities, and on-chain entities. The actions include off-chain actions and on-chain actions.

Users: Users are the real-world people who participate in the NFT ecosystem. Typically, users could be classified into three types according to their roles: creators, traders (sellers and buyers), and token owners.

On-chain entities: On-chain entities include NFT and marketplace smart contracts. The former implement the functionality (transfer, approval, etc.) of NFT tokens and the latter provide users with the ability to trade their NFTs.

Off-chain entities: Off-chain entities exist as a bridge between users and on-chain entities to improve usability and help visualize the assets represented by the NFT tokens. There are two types of off-chain entities. The first one is the front-end web applications that help users to perform NFT transactions, such as token transfer, approval, trading, etc. For example, the buyer can interact with the web application to choose the collection he or she wants to buy. Then the application will construct and sign the transaction with the user's private key (with the help of a wallet) and send it to the blockchain to execute the trading process. The second one includes digital assets and the storage service for the assets. An NFT token is usually associated with a digital asset that makes the NFT "meaningful". The digital asset is stored in an external storage server (usually the distributed storage file system IPFS or traditional centralized servers).

On-chain actions: On-chain actions are executed on the blockchain. As Fig. 1 shows, when the NFT contract receives the transfer transaction, it transfers the ownership of the token to the receiver. When the marketplace contract receives a swap transaction, it will complete the trading process.

Off-chain actions: Off-chain actions are performed among off-chain entities. As Fig. 1 shows, creators can create digital assets and store them in external storage servers. Minters (typically the same as creators) could mint NFT tokens and set their tokenURIs to the locations of the digital assets. Also, the users can pay to mint an NFT token and transfer the token to themselves.

Users usually interact with the web applications to construct the trade, transfer, or mint transactions. However, experienced users could directly interact with smart contracts on the blockchain.

1.2 Motivation of This Research

The NFT ecosystem is thriving in recent years. As Fig. 2 shows, the number of NFT contracts has been increasing speedily since 2021, and its popularity will remain in the foreseeable future. The NFT ecosystem has witnessed its value. According to NFTGo, the total valid trading volume (without wash trading) of the NFT ecosystem has exceeded $35.6B and the number of active users has reached $2.9M.

However, the emerging market has not been scrutinized to prove its reliability and stability. Poor protocol design and implementation may put users' assets at risk. Security incidents that caused huge financial losses have occurred in reality. For instance, the Akutar NFT contract has vulnerabilities that caused a 34M USD loss. With more funds flowing into the NFT ecosystem, security becomes more and more important.

In this report, we will systematically discuss security issues involved in the NFT ecosystem, which can be categorized into the following two types. The first one is the off-chain threat introduced by the off-chain actions and the second one is the on-chain threat introduced by the on-chain actions. We will discuss these two types of risks and report our analysis results in Section 3 and Section 4.

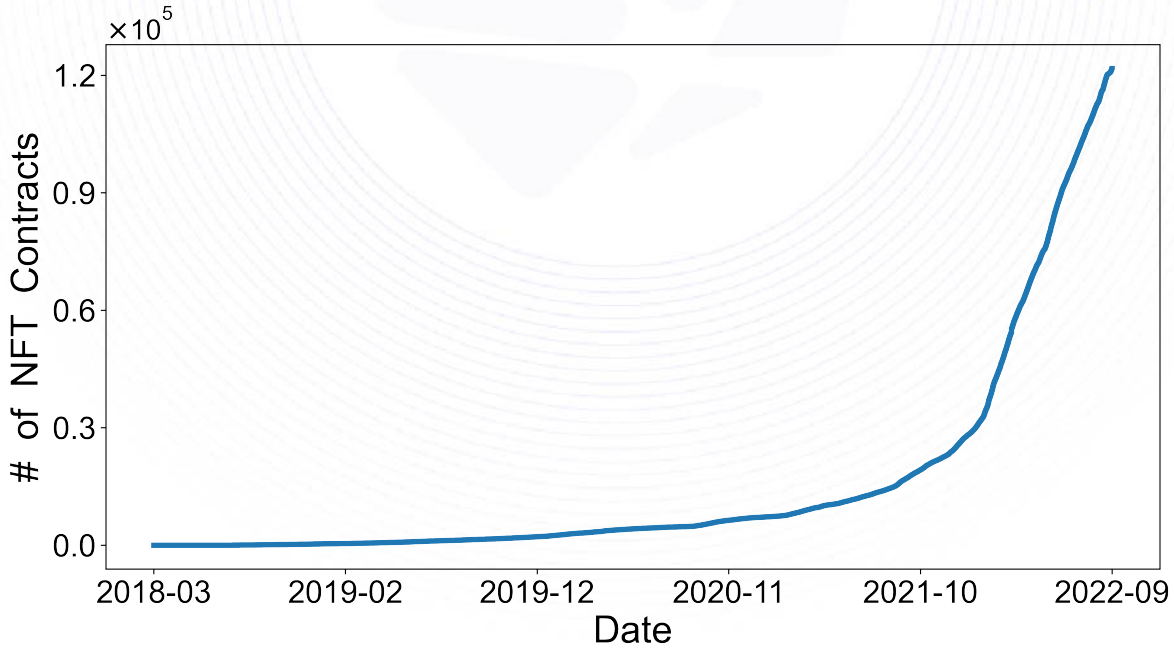

Fig. 2: NFT contracts growth on Ethereum.

2. Background

ERC-721. The ERC-721 standard is the most popular standard to implement NFT smart contracts. It defines the interfaces of an NFT token, as shown in listing 1.

Specifically, the ERC-721 protocol provides three events and twelve functions (another three functions are optional, i.e. **metadata extension**), which are applied to token control, data record (e.g. token transfer information), etc. Each NFT has an ID (**tokenId**), which identifies its uniqueness. Also, a map data structure is maintained in the token contract to record each NFT token's owner.

Basically, the token contract provides the **transfer** and the **approval** interface. The token owner could directly transfer the ownership to others (**transfer**) or grant others to spend his tokens on behalf of himself (**approve**). At the very beginning, NFTs should be minted. The mint process declares the existence of a token, and then the token could be used.

```
// standard ERC-721 protocols
    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);
// metadata extension is OPTIONAL for ERC-721
    function name() external view returns (string _name);
    function symbol() external view returns (string _symbol);
    function tokenURI(uint256 _tokenId) external view returns (string);
```

Listing 1: ERC-721 protocol.

When a token is minted, the contract records its **tokenId** and owner. Besides, metadata could be optionally specified and recorded on the blockchain. Most NFTs are used to represent assets in reality or digital collections that may have attributes that are recorded off the blockchain. The ERC-721 metadata extension provides the **tokenURI** method to connect between on-chain tokens and the corresponding off-chain assets. In particular, each token has a **tokenURI**, which is a URI referring to a JSON object to record the asset properties, i.e., the real address of the asset.

Fig. 3 shows an example of Mekaverse that supports the metadata extension. The tokenURIs of all meka tokens are recorded in the Mekaverse contract (on the blockchain). The tokenURI of meka #10 is in the IPFS format and refers to a JSON object that is meka #10's metadata. The "image" field in the metadata points to the location where the digital asset of meka #10 is stored.

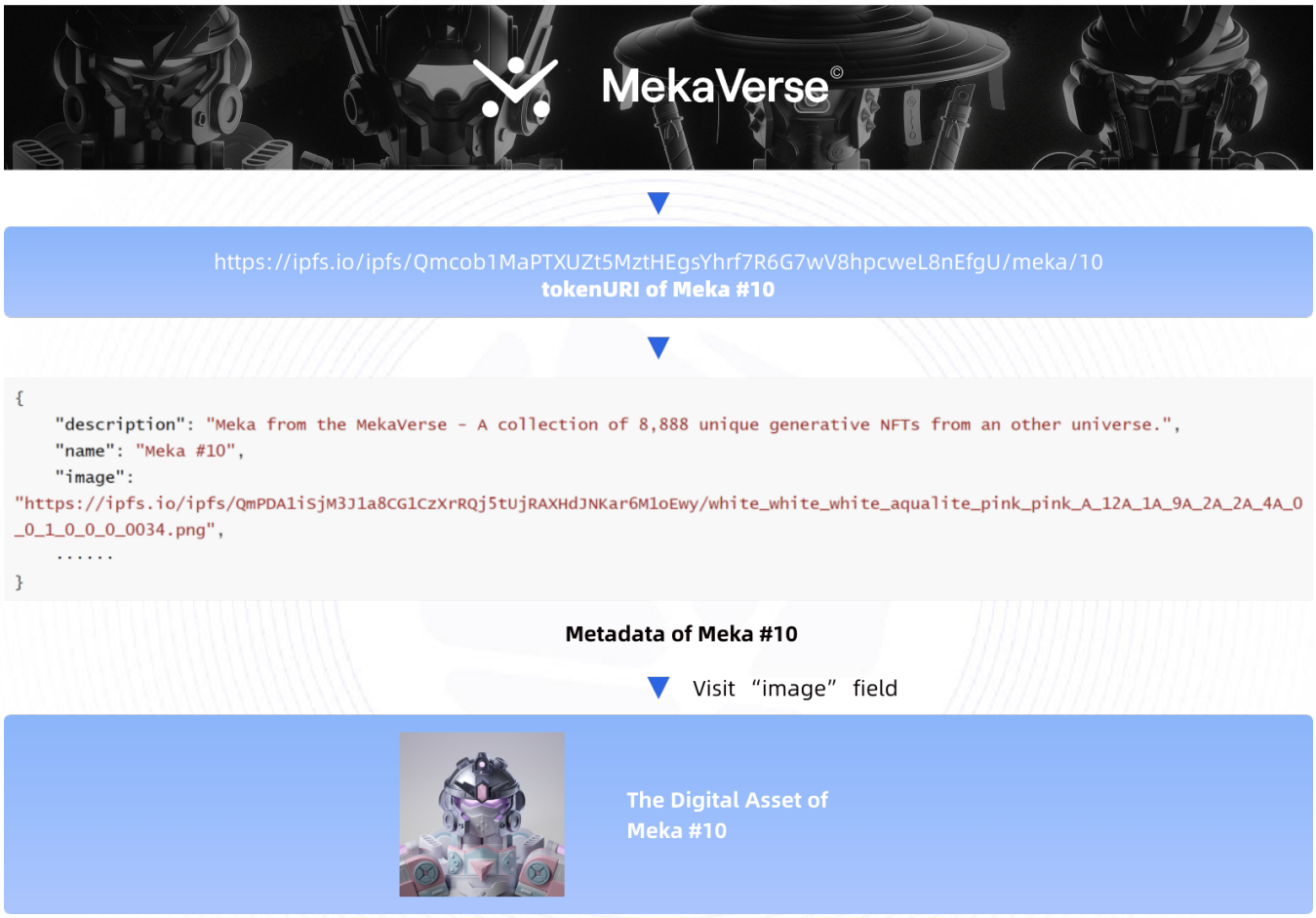

Fig. 3: The metadata of Mekaverse #10.

ERC-1155. The ERC-1155 multi-token standard is another standard to implement NFT smart contracts. The only difference between ERC-721 and ERC-1155 is that ERC-1155 allows fragmented tokens. That means one token could be split into many identical fragments. In another word, ERC-1155 is a "combination" of ERC-20 and ERC-721.

Marketplace. NFT marketplaces are Dapps, in which NFTs can be traded by users. Typically, an NFT marketplace consists of two parts, including front-end web applications for user interaction and on-chain smart contracts for trading process execution. NFT markets play a significant role for NFT users. They provide the trading functionality of NFTs and refine the financial attributes of NFTs. Users trade their NFTs on marketplaces and pay tax fees (mostly 0% ~ 5%) to marketplaces and NFT creators. Table 1 shows the information of the four largest marketplaces (responsible for more than 99% of trading volume).

Table 1: NFT marketplaces. Source: NFTGo.io

Marketplace	Trading volume	Users	Tax fee rate
OpenSea	$32.4B	2.1M	2.5%
LooksRare	$26.9B	115.3K	2.0%
X2Y2	$2.9B	100.1K	0.5%
CryptoPunks	$2.9B	6.9K	0.0%

Currently, most NFT marketplaces (e.g. OpenSea, LooksRare, and X2Y2) use the order-book trading mechanism. Meanwhile, to save the transaction cost (gas fee), the order verification is processed on the blockchain while the signing of the order is off the blockchain.

3. Methodology

Our research takes the following methodology as shown in Fig. 4. It consists of two stages: data collection and risk detection.

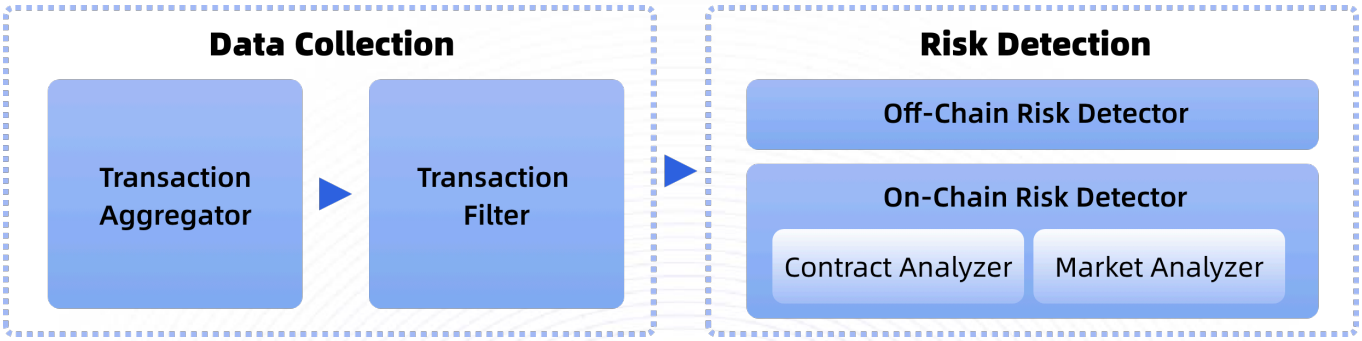

Fig. 4: The framework of the NFT risk detection.

3.1 Data Collection

The data collection stage is performed by two modules: transaction aggregator and transaction filter.

Transaction aggregator. We first use EthScope to download the Ethereum blocks and parse the blocks to output the semantic information of all transactions.

Transaction filter. The transaction filter parses the transactions and filters out the NFT events. It also queries the blockchain to maintain the status of NFT tokens and crawls from the Etherscan to collect the source code of NFT contracts. It finally generates the following information, including NFT trades information (seller, buyer, price, platform, etc.), ERC-721 token actions, NFT contracts and their source code (if open-source), and a real-time ERC-721 token status table that records the detailed token information, e.g., owner, tokenURI.

The event signatures used to extract the events are shown in Table 2.

Table 2: Event signatures for transaction filter.

Contract type	Contract name	Event name	Event Signature	Action type
ERC-721 & ERC-1155		Approval	0x8c5be1e5	Token approve
		ApprovalForAll	0x17307eab	
		Transfer	0xddf252ad	Token transfer
ERC-1155		TransferSingle	0xc3d58168	
		TransferBatch	0x4a39dc06	
Marketplace	OpenSea	OrdersMatched	0xc4109843	NFT trade
		OrderFulfilled	0x9d9af8e3	
	LooksRare	TakerAsk	0x68cd251d	
		TakerBid	0x95fb6205	
	X2Y2	EvInventory	0x3cbb63f1	
		EvProfit	0xe2c49856	

Dataset. The dataset contains data from July 2015 (Ethereum genesis block) to August 2022, including more than 15M blocks on Ethereum. An overview of the dataset is depicted in Table 3. Specifically, we collected 119.9K NFT contracts. Based on these smart contracts and their transactions, we extracted 83.1M ERC-721 tokens with token information (owner, tokenURI, mint time, etc.) and token actions (mint, transfer, and burn).

We also monitored the top three NFT marketplaces: OpenSea, LooksRare, and X2Y2, and collected 25.9M trade transactions in these marketplaces. OpenSea is the biggest NFT marketplace and occupies most NFT trades (95%). LooksRare and X2Y2 are two rising NFT marketplaces in 2022 and also attract many NFT traders.

Table 3: The overview of the dataset.

# of NFT contracts		# of ERC-721 tokens	# of trades	
Total	119.9K	83.1M	Total	25.9M
ERC-721	104.2K		OpenSea	24.6M
ERC-721 with assets	84.8K		LooksRare	0.3M
ERC-1155	15.7K		X2Y2	1.0M

3.2 Risk Detection

The risk detection is to detect the off-chain risks (by the off-chain risk detector) and the on-chain risks (by the on-chain risk detector).

Off-chain risk detector: The off-chain risk detector collects the information of off-chain entities, including the token metadata and digital assets. It takes the NFT token information and tokenURIs as inputs and monitors the accessibility of the off-chain assets. It accesses the metadata of NFT tokens from the tokenURIs, then resolves the metadata to extract the locations where the tokens' digital assets are stored. If the assets cannot be accessed, then the users who own these tokens are under the inaccessibility risk.

On-chain risk detector: The on-chain risk detector monitors the on-chain NFT contracts and activities, takes the NFT source code and NFT activities as inputs, and detects the contract-related risks by the contract analyzer as well as the market-related risks by the market analyzer. The contract analyzer detects the risks introduced by the implementation of NFT smart contracts, such as contract vulnerabilities and contract backdoors. The market analyzer detects the malicious market behaviors of the NFT ecosystem, including holder pooling (token hoarding) and wash trading.

4. Detailed Result

4.1. Off-Chain Risk

The off-chain risk is introduced by the off-chain assets security issues. it concerns the accessibility of the off-chain asset.

As previously explained, many NFT tokens are associated with off-chain assets that are stored in external storage servers. The value of an NFT token is endorsed by its corresponding asset, instead of the token itself. The accessibility of the assets should always persevere as long as the tokens exist to maintain the consistency between the on-chain tokens and the off-chain assets. Once the off-chain assets become inaccessible, the corresponding tokens owned by users become worthless.

Table 4: The accessibility of ERC-721 NFT assets.

	Accessible	Inaccessible
# of NFT projects	68.7K (81.0%)	16.1K (19.0%)
# of NFT tokens	48.9M (90.6%)	5.1M (9.4%)
Est. value (in Ether)	5099.4K (93.9%)	330.2K (6.1%)

To understand the overall result of the accessibility of NFT assets, we checked 84.8K ERC-721 NFT projects with 54.0M tokens that support metadata extension and have corresponding digital assets. That means there exists an “image” field or “image_url” field in the token metadata. Our experiment was performed on August 30, 2022.

Table 4 shows the detailed accessibility result of the NFT assets. Assets in around 19.0% of the NFT projects (with 5.1M tokens) can not be accessed. This implies that the value of these tokens cannot be preserved.

We further evaluate the market value of these inaccessible tokens. To be simple, we use Ether to be the currency when talking about the NFT’s price. The last trade price of a token could be considered as its estimated value. For a token that has never been traded, its estimated value is 0. Our analysis shows that the value of inaccessible assets is around 330.2K Ether (about USD 515.1M in terms of the Ether price being USD 1,550 on August 30, 2022). This causes a huge financial loss to their owners.

4.2. On-Chain Risk

The on-chain risks are introduced by the vulnerabilities or malicious logic in the contracts (contract risk), and the abnormal market behaviors that may lead to financial losses (market risk).

4.2.1 Contract Risk

The contract risk refers to the risks introduced by the improper design and implementation of NFT smart contracts, including vulnerabilities and backdoors in NFT smart contracts. Our research focuses on the following types of vulnerabilities and malicious logic.

Contract transparency. The NFT smart contracts deployed on the blockchain should be open-sourced and/or publicly audited to maintain transparency and credibility. As Table 5 shows, while most NFT contracts (85.1%) are open-sourced, there are still a few NFT contracts (14.9%) that are closed-source.

Table 5: Transparency of NFT contracts.

# of NFT contracts	# of open-source	# of closed-source
119,891	102,060 (85.1%)	17,831 (14.9%)

Reentrancy vulnerability. In our previous blog, we reported a security incident caused by a reentrancy vulnerability in the NFT smart contract and analyzed the root cause of this attack. It is caused by the _safeMint function in the contract.

Improper access control vulnerability. The NFT contracts provide users with the ability to mint and transfer their tokens. But the operations should be authenticated (and authorized). For example, a user should not burn others' tokens (that do not belong to himself/herself). If developers do not perform proper access control to critical (public) functions, the authorization and authentication mechanism can be bypassed. Listings 2 and 3 show examples of such vulnerabilities in NFT contracts.

Privilege function. The Privilege function is the function that only allows privileged users (mostly contract owners) to execute some critical actions that may cause damage to users. Listings 4, 5, and 6 show examples of privilege functions.

```
function safeTransferFrom(address from, address to, uint256 tokenId, bytes memory _data)
        public virtual override {
    _checkOpenTransfer(from, to, tokenId);
    _safeTransfer(from, to, tokenId, _data);
}

function _checkOpenTransfer(address from, address to, uint256 tokenId) internal {
    if (_isApprovedOrOwner(_msgSender(), tokenId)) { return; }
    emit OpenTransfer(msg.sender, from, to, tokenId);
```

Listing 2: An example of public transfer. Although the _checkOpenTransfer function checks the approval status, it does not return a boolean variable to tell the safeTransferFrom function whether the operator (the caller of this function) has the privilege to transfer the owner's token or not. In another word, any user could transfer the other user's tokens without their consent.

```
function burn(uint256 tokenId) external {
    require(_exists(tokenId));
    _burn(tokenId);
}
```

Listing 3: An example of public burn. The burn function only checks the existence of the burned token without checking the owner of the burned token to be identical to the caller. The result is that anyone could burn any tokens, despite that he does not own the tokens.

```
// for normal users
function claim(uint256 tokenId) public payable nonReentrant {
    require(tokenId > 0 && tokenId < 7778, "Token ID invalid");
    require(mintPrice <= msg.value, "Please pay mint fee");
    _safeMint(_msgSender(), tokenId);
}

// for privileged users
function ownerClaim(uint256 tokenId) public nonReentrant onlyOwner {
    require(tokenId > 7777 && tokenId < 8001, "Token ID invalid");
    _safeMint(owner(), tokenId);
}
```

Listing 4: Normal mint function and privilege mint function. Normal users could only use the function claim to mint tokens by paying the mint fee. But the function ownerCliam allows the contract owner to arbitrarily mint tokens without any cost. This may cause token inflation. Note that the onlyOwner modifier requires that the ownerClaim function could only be invoked by the contract owner.

```
function safeTransferNFT(address from, address to, uint256 tokenId)
        public onlyOwner {
    _safeTransfer(from, to, tokenId, "");
}
```

Listing 5: Privilege transfer function. The function allows the contract owner to arbitrarily transfer others' tokens, despite that the contract owner does not own the tokens.

```
function _isApprovedOrOwner(address spender, uint256 tokenId)
        internal view virtual returns (bool) {
    address owner = ERC721C.ownerOf(tokenId);
    return (spender == owner || getApproved(tokenId) == spender
            || isApprovedForAll(owner, spender) || _superOperators[_msgSender()]);
}
```

Listing 6: Privilege _isApprovedOrOwner function. If the contract owner is the token spender, the _isApprovedOrOwner will always return true to indicate that the approval status is valid, which means the function _isApprovedOrOwner grants the contract owner the privilege to spend other users' tokens without their consent.

Sleepmint. Privilege functions can be leveraged to perform an interesting social engineering attack called sleepmint. A typical process of sleepmint is: 1) An attacker creates an NFT contract with privilege functions by which he could spend any tokens without the owners' permission. 2) The attacker mints a token to a high-profile person (without his/her consent). This makes an impression that the high-profile person holds the NFT token. 3) Later, the attacker exploits the privilege function to transfer the token back to his account and list the token on the marketplace. This makes other users believe that the token is valuable because the token has been minted to and/or held by a high-profile person. The victims may be tripped to buy the token from the attacker's account.

The result. We found that 56,519 (55.4%) out of 102,060 open-source NFT smart contracts have contract risks. The detailed analysis results are shown in Table 6. 4,401 (4.3%) NFT contracts have vulnerabilities (reentrancy and/or improper access control). 54,549 (53.4%) NFT contracts have the privilege functions, such as privilege mint, privilege burn and privilege transfer, etc. Our study also found 75 NFT contracts involving sleepmint behavior (with 1,960 transactions).

Table 6: Statistics of contract risks.

Type	# of contracts	Percentage
Total	102,060	100.0%
Vulnerability	4,401	4.3%
Reentrancy	4,284	4.2%
Improper access control	135	0.1%
Privilege function	54,549	53.4%
Sleepmint	75	0.7‰

4.2.2 Market Risk

The market risk lies in the abnormal on-chain market behaviors, e.g. **holder pooling and wash trading.**

Holder pooling. Holder pooling refers to the circumstances that few users (also called "big whales") hold most tokens in an NFT project. This introduces the risk of ownership concentration.

"The capital structure is highly related to the corporate performance and market index in traditional finance, and over-centralized ownership may depress the market evolvement". This concept is also applicable to the NFT market, as one could hold considerable tokens of an NFT project to control the market.

Typically, the health of an NFT market is related to its liquidity and degree of token distribution. High liquidity and strong dispersion help build a robust and financial risk-resisting ecosystem. Holder pooling risk is raised when the distribution of NFT tokens is too concentrated and further there is a risk of pump-and-dump.

Fig. 5 shows the holder distribution of three popular NFTs, which presents a low risk of holder pooling as no one controls most of the NFT tokens. Fig. 6, in contrast, shows that one address controls more than 50% of NFT tokens. The "big whales" could manipulate the NFT market, leading to financial risks to the NFT market. Table 7 shows the detailed statistics.

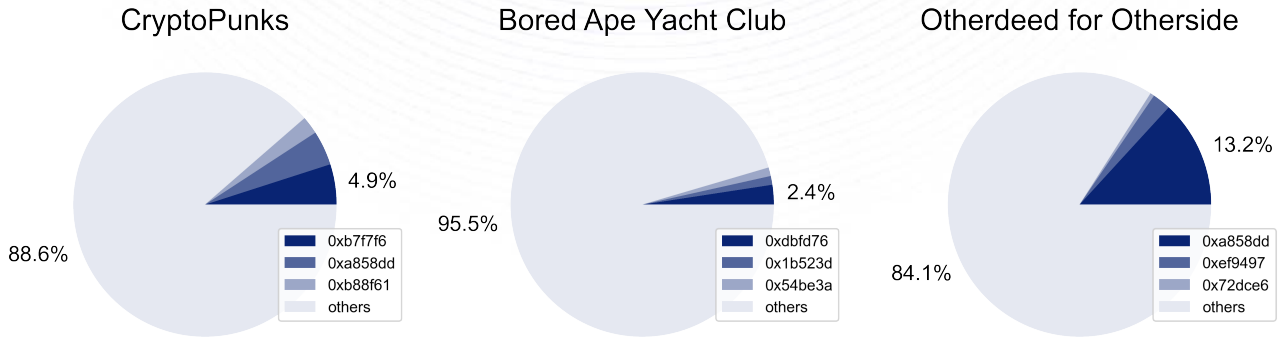

Fig. 5: Holder distribution of top three NFTs.

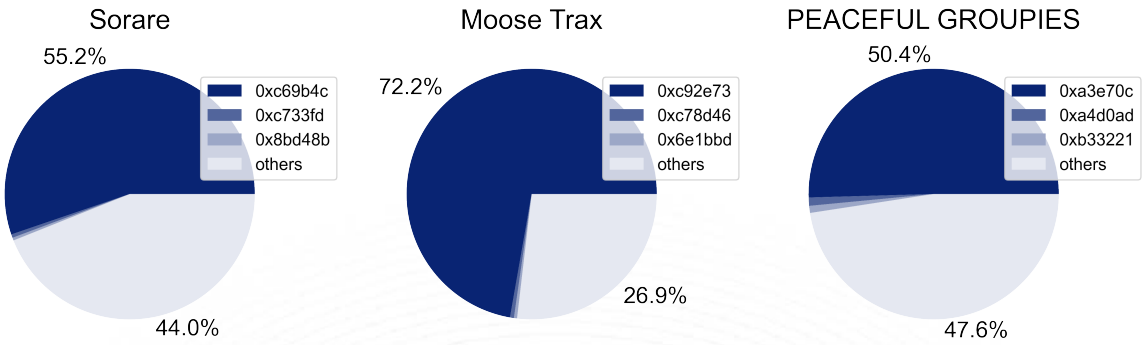

Fig. 6: Holder distribution of three NFTs with holder pooling risk.

Table 7: Statistics of holder distribution.

NFT name	Address	Total supply	Biggest whale	Holding count	Percentage
CryptoPunks	0xb47e3cd837ddf8e4c57f05d70ab865de6e193bbb	9,998	0xb7f7f6	493	4.9%
Bored Ape Yacht Club	0xbc4ca0eda7647a8ab7c2061c2e118a18a936f13d	9,998	0xdbfd76	241	2.4%
Otherdeed for Otherside	0x34d85c9cdeb23fa97cb08333b511ac86e1c4e258	100,000	0xa858dd	13,164	13.2%
Sorare	0x629a673a8242c2ac4b7b8c5d8735fbeac21a6205	331,445	0xc69b4c	182,911	55.2%
Moose Trax	0x3146dd9c200421a9c7d7b67bd1b75ba3e2c15310	7,723	0xc92e73	5,578	72.2%
PEACEFUL GROUPIES	0x4f89cd0cae1e54d98db6a80150a824a533502eea	9,998	0xa3e70c	5,040	50.4%

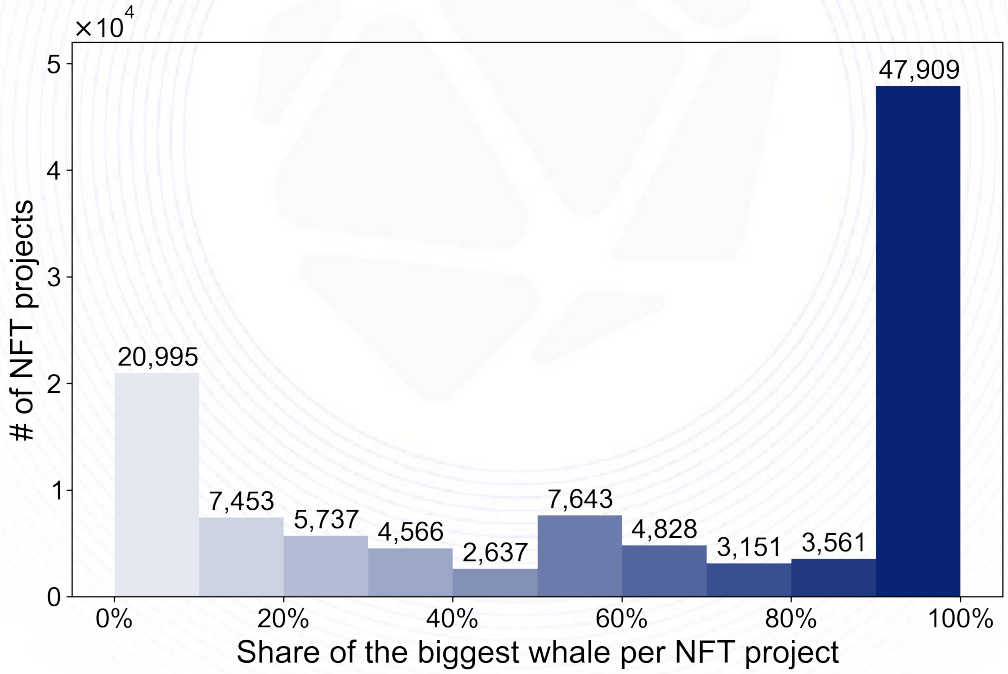

Fig. 7: The shares of the biggest whales of NFT projects.

To understand the overall result of the holder distribution of NFTs, we checked the shares of the biggest whales of the 108.5K ERC-721 NFT projects. The histogram in Fig. 7 shows the polarisation of the holder distribution of NFTs. Surprisingly, 47,909 (44.2%) NFT projects are extremely centralized since one user (the biggest whale) holds more than 90% of the tokens in these projects.

To be simple, we define an NFT project at holder pooling risk if more than 50% of its tokens are controlled by its biggest whale, i.e. the share of the biggest whale of the NFT project exceeds 50%. The result shows that 67,092 (61.8%) NFT projects are suffering from the holder pooling risk.

Wash trading. Wash trading, also called Round Trip Trading, Wash Sales, is defined as "Entering into, or purporting to enter into, transactions to give the appearance that purchases and sales have been made, without incurring market risk or changing the trader's market position." by the U.S. Commodity Futures Trading Commission (CFTC). The U.S. Commodity Exchange Act prohibits wash trading. A wash trade, to be simply, in the NFT market is a form of market manipulation in which a user simultaneously sells and buys the same NFT collections to create misleading, artificial activity in the marketplace. A major purpose of wash trading is to artificially increase trading volume, giving the impression that the collection is in higher demand than it actually is, i.e. hype. Due to the lack of regulation, the current NFT market has many wash trading transactions, which may cause a continuing financial bubble.

Fig. 8 shows an example of wash trading taken in LooksRare (Terraforms #9728 on the Ethereum). The collection is traded between two addresses with high prices. These behaviors directly increase the trading volume, which may mislead the activity of the NFT. In fact, the trading market of Terraforms is filled with wash trading with the wash trading exceeding $2.9B, according to Andrew Hayward's analysis.

Txn Hash	Age	Action	Price	From	To
0x005a70a5cd5b0137e1...	3 days 56 mins ago	Bid Won	250 WETH ($457,307.50)	0xa53496b67eec749ac4...	0xd73e0def01246b650d...
0x574c436ecf468616be...	8 days 16 hrs ago	Bid Won	639.6264 WETH ($1,170,023.80)	0xd73e0def01246b650d...	0xa53496b67eec749ac4...
0xfa44ce13d43acba68c5...	9 days 14 hrs ago	Bid Won	639.6264 WETH ($1,170,023.80)	0xa53496b67eec749ac4...	0xd73e0def01246b650d...
0x34037dc70467fb2fc18...	14 days 6 hrs ago	Bid Won	812 WETH ($1,485,334.76)	0xd73e0def01246b650d...	0xa53496b67eec749ac4...
0x4f2fabf7e6a4e7e4548f...	14 days 6 hrs ago	Bid Won	864 WETH ($1,580,454.72)	0xa53496b67eec749ac4...	0xd73e0def01246b650d...
0x36891385433640ca43...	15 days 3 hrs ago	Bid Won	416.9 WETH ($762,605.99)	0xd73e0def01246b650d...	0xa53496b67eec749ac4...
0xa1acda9b54de6500cc...	16 days 4 hrs ago	Bid Won	436 WETH ($797,544.28)	0xa53496b67eec749ac4...	0xd73e0def01246b650d...
0xc88e06adfbb1245e46...	16 days 4 hrs ago	Bid Won	475 WETH ($868,884.25)	0xd73e0def01246b650d...	0xa53496b67eec749ac4...

Fig. 8: An example of wash trading.

We have analyzed the activities of the top three NFT marketplaces (OpenSea, LooksRare, and X2Y2) and used an algorithm to detect the wash trading activities over the past year (Apr. 2021 ~ Apr. 2022). The key point of the detection algorithm is to find "cycle trades". The whole detection process is as follows: First it establishes the NFT trade graph *G(V, E)*. The graph is a directed multigraph where *V* is the set of traders and *E* is the set of trades. The direction of each

edge is from the NFT token seller to the NFT token buyer. Then it finds the cycle trade relations (cyclic sub-graph) which are considered as wash trading activities.

To decrease the false positives, we use the degree of graph threshold to improve the precision of the detection. In a directed multigraph G, we denote the degree of the graph d(G) as "The minimum of the in-degrees and out-degrees of all vertices of the graph". For example, Fig. 9 shows that the left graph's degree is one and the right graph's degree is two. The degree of a cyclic trade graph could reflect the wash trading probability. The larger the d(G), the more likely the trades are wash trading. Here we heuristically set the threshold of d(G) = 3: For any cyclic trade graph G with d(G) > 3, the trades could be taken as wash trading.

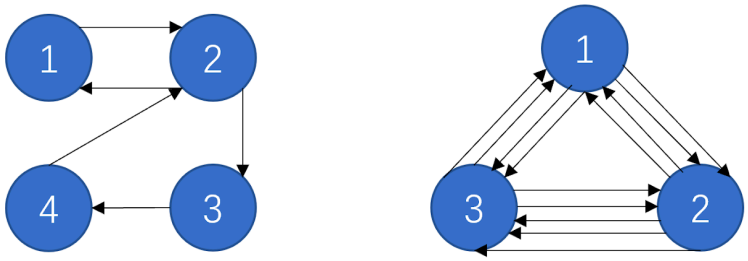

Fig. 9: The left graph's degree is one and the right's is two.

Our analysis is based on the trading currency as Ether (the Ethereum's native token), i.e. we only consider the trading between NFTs and Ether. Table 8 shows that 205 NFT projects and 14K traders are involved in wash trading.

Table 8: Statistics of wash trading NFT projects.

# of NFT projects with wash trading	# of wash traders
205	1412

Table 9 shows the statistics of the wash trading on the top three NFT marketplaces. The total wash trading volume reaches 9.8M Ether and the ratio reaches 43% compared with the total trading volume. For LooksRare and X2Y2, over half of the trading volume on the two platforms are wash trading (LooksRare: 87.5%, X2Y2: 72.2%). Most wash trading is happening on LoosRare as it occupies 85.7% of the total wash trading volume (Total: 9.8M, LooksRare: 8.4M). Table 10 shows the top ten wash trading NFTs.

Table 9: Statistics of wash trading on top three marketplaces.

Platform	# of total trades	# of wash trades	Total trading vol. (in Ether)	Wash trading vol. (in Ether)	Wash trading vol. percentage
Total	25.9M	44.4K	22.8M	9.8M	43.0%
OpenSea	24.6M	7.2K	11.4M	0.1M	0.9%
LooksRare	0.3M	22.4K	9.6M	8.4M	87.5%
X2Y2	1.0M	14.8K	1.8M	1.3M	72.2%

Table 10: Top ten wash trading NFTs.

NFT Name	NFT address	Wash trading vol.	Total trading vol.	Percentage
Terraforms	0x4e1f41613c9084fdb9e34e11fae9412427480e56	4.21M	4.26M	98.8%
Meebits	0x7bd29408f11d2bfc23c34f18275bbf23bb716bc7	3.0M	3.6M	84.0%
dotdotdot	0xce25e60a89f200b1fa40f6c313047ffe386992c3	923.3K	975.5K	94.6%
More Loot	0x1dfe7ca09e99d10835bf73044a23b73fc20623df	643.9K	648.0K	99.4%
Dreadfulz	0x81ae0be3a8044772d04f32398bac1e1b4b215aa8	248.1K	416.9K	59.5%
CATGIRL ACADEMIA	0xa5d37c0364b9e6d96ee37e03964e7ad2b33a93f4	149.9K	150.0K	99.9%
Audioglyphs	0xfb3765e0e7ac73e736566af913fa58c3cfd686b7	137.0K	138.1K	99.2%
Loot	0xff9c1b15b16263c61d017ee9f65c50e4ae0113d7	93.6K	304.9K	30.7%
CryptoPhunksV2	0xf07468ead8cf26c752c676e43c814fee9c8cf402	84.3K	86.5K	97.5%
dementorstownwtf	0xff36ca1396d2a9016869274f1017d6c2139f495e	77.7K	78.9K	98.5%

Our analysis also indicates that 87.5% of the trading volume on LooksRare is wash trading. This compiles with a third-party analysis by JP Buntinx. An interesting perspective is that the purpose of wash trading on LooksRare is not merely inflating the trading volume or price. In our previous post, we found the practice of wash trading to arbitrage on LooksRare: Users constantly trade their NFT tokens back and forth between their own Ethereum accounts to earn trade rewards (LOOKS or WETH).

Note that our analysis is conservative. The algorithm is simple as it does not consider address clustering. The most straightforward pattern for wash trading is repeated trading between only two addresses, which is easy to identify. However, users could control multiple addresses or collude with others to hide malicious trades and avoid being tracked. Our algorithm found out that more than 10M Ether trading volume is wash trading, but this is only the "tip of the iceberg" as more wash trading is hidden beneath the surface. As wash trading disrupts the order of the NFT ecosystem, we will continue to focus on wash trading detection, improving the detection performance by address cluster, account entity identification, etc.

5. Discussion

There exist other risks that our report does not cover, which we will discuss in this section.

Asset integrity risk. The blockchain technology only guarantees the integrity of on-chain data but not off-chain data. Many NFT assets are stored on centralized servers. The server owner could modify assets without anyone's notification. Meanwhile, the assets stored on centralized servers may be tampered due to the servers' crashes or attacks.

Copyright & royalty risk. NFTs provide creators and collectors with the ability to create and trade their digital assets. The whole process is transparent and immutable. However, such a mechanism also introduces the copyright issue. A user could steal others' creations to mint an NFT and then trade for profits.

Phishing & scam risk. Social engineering attacks also exist in the NFT ecosystem. Phishers and scammers trick users to steal users' private keys and/or deceive victims into signing malicious transactions.

On April 1, 2022, the pop star Jay Chou lost his Bored Ape Yacht Club #3738 (**155 Ether**). The root cause is that his private key was stolen by a phishing website; In May 2022, 29 Moonbirds tokens valued at $1.5M were stolen by hackers in a phishing attack.

Fig. 10: Jay Chou's post (left), and the lost Moonbirds (right).

In fact, phishing and scams are very popular: "Discord has been targeted by hackers over the last three months with increasing frequency. In June 2022, phishing attacks linked to NFT minting scams deployed through compromised Discord accounts increased by 55% in comparison to the previous month. The NFT community has lost an estimated $22 million since May 2022", According to a report by TRM Labs.

6. Security Tips

In this section, we will propose some security tips for NFT users to protect their NFTs.

6.1 To Avoid the Off-Chain Risk

Check the accessibility of assets. Once you buy an NFT token, you should check the accessibility of your assets from time to time. If you find that your assets can not be accessed, you should stop investing in the NFT to prevent further loss.

Investigate before investing. Scrutinize the overall image of the project, check the reputation of the teams and the community liveness of the communities. In general, the fame of a team guarantees the value of the assets.

6.2 To Avoid the On-Chain Risk

Invest in audited projects. Smart contract auditing is a necessary process that scrutinizes codes to identify contract risks.

Be aware of abusing the approval mechanism. The approval mechanism grants blanket authorization to third-party accounts to operate on your assets. If the Dapps that you approve get compromised, your tokens will be at risk... Do not approve your tokens to untrusted third-party accounts. When you want to revoke your approvals, this tool https://revoke.cash/ can help you.

Check the holder distribution. Do not invest in the NFTs where most tokens are controlled by a few accounts. If few accounts control most tokens, the few accounts can manipulate the market price easily. Try to invest in those NFTs whose tokens are held scattered. The holder information of an NFT project can be accessed on the NFT Go website. Here is an example of the BAYC holder information.

Identify wash trading. The wash trading phenomenon may mislead you in judging the value of NFTs. It is important to distinguish the wash trading volume and the real trading volume. NFT Go develops a tool that can help you filter the wash trading activities, The guide can be accessed here.

6.3 Others

Besides, some general security tips help avoid both off-chain and on-chain risks.

Do not share your private keys or recovery phases with anyone. As the popular crypto saying goes, "not your keys, not your coins". Giving your keys or phases to others means that they can operate on your assets.

Interact with only official sites, such as official websites or official Discord. Many incidents occurred because victims visited phishing or scam websites where attackers steal their private keys. Do not interact with any untrusted external websites and social accounts. Here are some tips for users to validate the Dapp websites:

- **Pay attention to the website address bar.** Only interact with **HTTPS** websites instead of **HTTP** websites. HTTPS uses TLS (SSL) to encrypt normal HTTP requests and responses and to digitally sign those requests and responses. As a result, HTTPS is far more secure than HTTP.
- **Carefully check the domain name.** One of the favorite tricks of hackers is to create a look-alike domain name to cheat careless uses. For example, a website domain name of https://opensea.io can be changed to https://opensae.io by reversing the letter “e” and letter “a”. Always double-check every letter of the domain name.
- **Distinguish the official and fake social media** (Twitter, Discord). Some attackers disguise official maintainers to cheat users.

Subscribe to official announcements and follow any security news. Keep up with any official security updates to make sure your assets' security is guaranteed. Meanwhile, pay attention to security incidents. If necessary, transfer your tokens to a safe account to protect your assets.

Check your transaction before sending and verify it after sending. Always make sure you understand the meaning of the transaction before sending and verify the result. Do not directly sign and send the transaction that you don’t understand, this may endanger your assets. Verify the status of your transaction, and make sure that the transaction is completed with your expectation.

7. Conclusion

This report systematically reveals the risks of the NFT ecosystem. We identify three entities and present the on-chain and off-chain risks of the NFT ecosystem. Our analysis shows that the security of the NFT ecosystem is worrisome, with inaccessible assets, vulnerable contracts, holder pooling tokens, and wash trading transactions. We will actively monitor the risks and share the latest result with the community to help build a more secure NFT ecosystem.

Contact Us

BlockSec

Mail: contact@blocksec.com
Website: https://blocksec.com/
Twitter: https://twitter.com/blocksecteam
Github: https://github.com/blocksecteam

NFTGo

Mail: social@nftgo.io
Website: https://nftgo.io/
Twitter: https://twitter.com/nftgoio
Mirror: nftgo.mirror.xyz