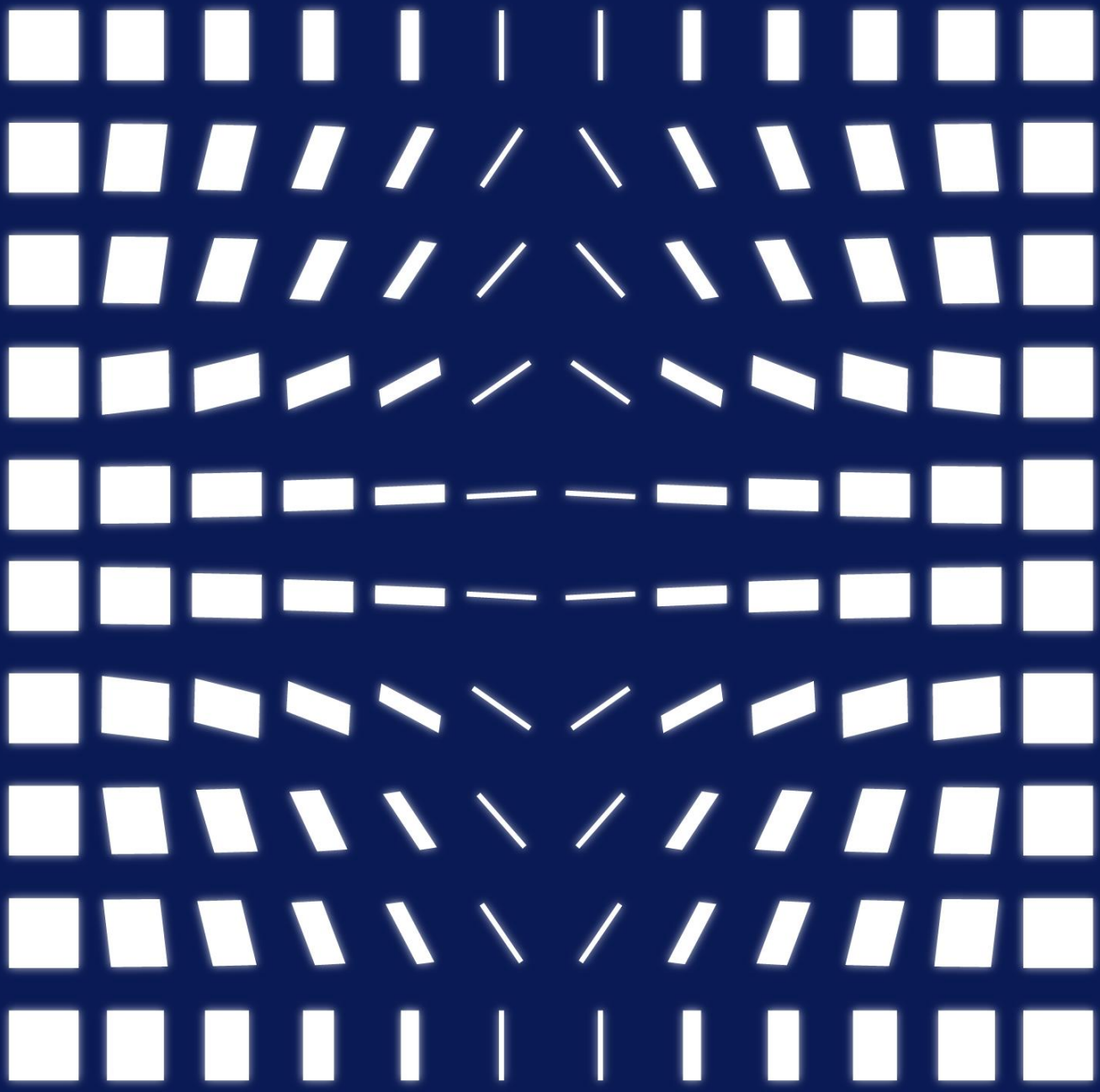
Huobi Research

The Advanced Road for NFT Standards



Author: Huobi Research Institute / Yeyan Wei

The Advanced Road for NFT Standards

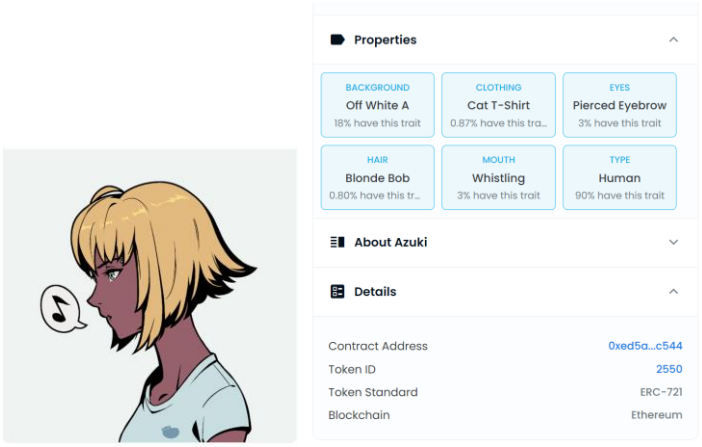
The Non-Fungible Token (NFT) market seems prosperous of late. The total traded volume for 30 days reached US$6.2B, according to data from NFTGO. Unlike other tokens, the minimum unit of NFT is 1, which means it cannot be split. The fundamental reason for determining the properties of these tokens is that they refer to different contract standards. The most common tokens, such as $APE tokens, are issued under the ERC-20 standard, which can be exchanged casually, as well as split and integrated. Unlike ERC-20, most NFTs follow the ERC-721 (Ethereum Request for Comments 721) standard, which is the standard implemented by most NFTs on Ethereum. Tokens under this standard are not exchangeable, which represents the uniqueness and irreplaceable nature of NFTs.

1. Unfairness under the ERC-721 standard

By understanding the ERC-721 standard itself, we can know how an NFT is issued, minted, and priced. There are already many NFT issuance platforms which can simply issue NFTs without know any coding knowledge. For example, on OpenSea, users only need a file (JPG, PNG, GIF, SVG, MP4, WEBM, MP3, WAV, OGG, GLB, GLTF) and a wallet to issue an NFT. Minting an NFT involves performing one operation and paying the gas fee once. If you wish to mint an NFT series, the gas fee needs to be paid multiple times. This is in accordance with the ERC-721 standard and obviously inconvenient for minting a series of NFTs.

All NFTs have a uint256 variable called tokenID. Contract address and uint256 tokenID represent an NFT's uniqueness in the entire blockchain. Only after the previous tokenID has been minted can the next tokenID start. In addition, NFTs have some properties that determine their rarity. Take Azuki as an example. There is a total of 10,000 NFTs that have been issued. Each NFT has 9 properties, including clothing, eyes, etc., and the project will set the probability

of various rare properties, resulting in a series of NFTs with different rarity levels. The rarer the NFT in the market, the higher its price.

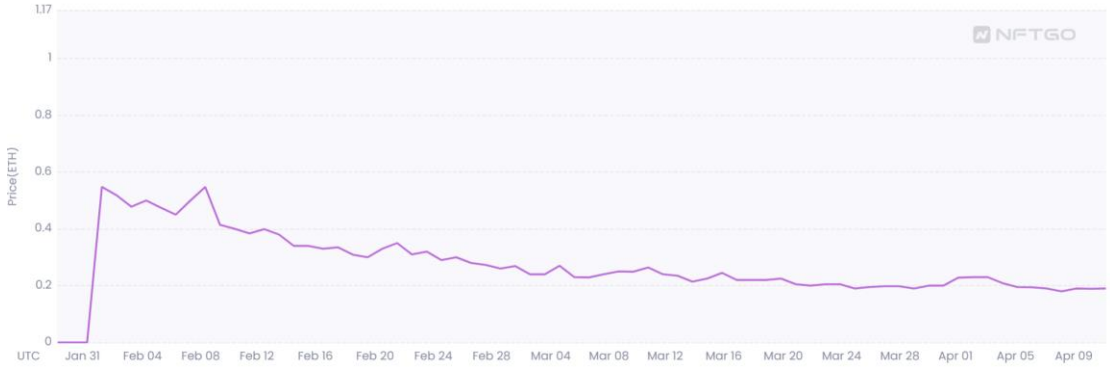


Graph.1 Azuki NFT #2550 properties and rarity

As a buyer, we hope to mint the rare NFTs when they are first issued. It feels akin to opening a mystery bag, which requires luck to obtain the one you want. But in the world of NFTs, sometimes getting the rare NFTs may not be related to luck. Shortly before the NFT series is about to be issued, project developers will put the NFT's tokenID and the metadata's storage address hash (may be IPFS hash) in the smart contract. This way, buyers have the opportunity to obtain the tokenID corresponding to the rare NFT before it is minted. An on-site bot can then be used to mint the NFT at the appropriate time to obtain the rare NFT.

In order to avoid the above situation, some projects will choose to randomly distribute NFTs with different properties according to the tokenID, after all NFT series products are completely minted. However, this means that users cannot know in advance whether this distribution is fair or not, because the right to issue NFTs lies in the hands of the project developers, which is centralized.

Except for NFT issuance and minting, the issuance and pricing patterns of NFTs are also full of tricks at present. The pricing right is totally controlled by the project side, and users only make purchase choices with limited information. This is likely to result in the highest price on the day of issuance, as shown in Graph.2. And this is also the general case for NFT price changes.



Graph.2 Floor Price of Angry Ape Army Evolution Collection (From: NFTGO)

The phenomenon of unfairness in the current NFT market described above may cause users to suffer property losses with the unequal distribution of information. There are also a lot of new projects trying to find solutions to these problems. For example, random allocation of NFTs in a more decentralized way, or actively build and empower NFT communities and establish whitelists. However, there are also some who envision new ERC standards that will help solve such problems.

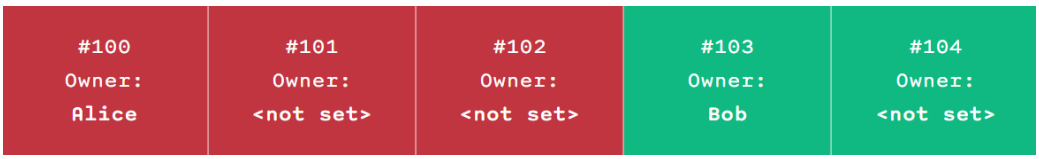
2. ERC-721A and Azuki's new gameplay

The floor price of the Azuki project has been increasing since January. Except for the operation of the community brand, the project side has bold and innovative ideas and acted on some of them. In order to solve the problem of paying more gas fees for minting multiple NFTs, Azuki proposed a new NFT standard: ERC-721A. This standard allows for the gas cost of minting multiple NFTs to be nearly equal to that of minting one NFT.

ERC-721 implements NFT minting by updating the data of the NFT holder's address according to each NFT. In ERC-721A, a batch of NFT is minted, and the holder's address is updated only once. This needs to meet two preconditions: 1. Confirm whether the user has enough balance to mint when the user proposes batch minting request; 2. The NFT minted in batch by the user is of a continuous tokenID. In addition, ERC-721A removes the redundant storage brought by ERC-721.

Implementation is also quite crafty. We shall use an example from the Azuki project's official introduction to illustrate this here. Alice minted NFTs numbered

#100, #101, #102, while Bob minted NFTs numbered #103, #104. Under the ERC-721A standard, it is only necessary to update the information of holders Alice and Bob under the NFTs of #100 and #103, respectively. If you wish to know the owner of #102, you just need to traverse to the nearest address, which would lead to the owner of #100. There will obviously still be risks, but Alice can always attach her own address to all her NFTs. In this way, we can avoid the problem of high gas fees. The real purpose of ERC-721A lies in saving gas fees for users, which is still a necessity for projects on Ethereum.



Graph.3 Alice and Bob batch mint

3. The Road Not Taken: ERC-721R

Currently, there are several standards called ERC-721R, which are some new NFT standards that have been hotly debated recently. Two of the most famous ones attempt to solve the above unfairness issues with ERC721: 1. ERC-721R proposed by exo-digital-labs provides trustless refunds; 2. ERC-721R proposed by erc721r.org provides a solution to the rare NFT distribution.

(1) **Trustless refund mechanism**

The ERC-721R standard proposed by exo-digital-labs aims to build a healthy and stable NFT ecosystem. It provides buyers with greater protection by offering a refund mechanism. The standard provides project designers with two parameters: the refund waiting period and the refund ratio. For NFT projects implemented under the ERC-721R standard, the funds spent by users will be managed by smart contracts, and the project designers will not be able to withdraw funds until the refund waiting period ends. During the waiting period, users can return their NFTs to the smart contract and get their ETH back at any time.

During the refund waiting period, the price of the returned funds will become the lowest price of the floor price, which can effectively guarantee the rights of investors. For buyers, there is a period of low risk, but after the waiting period, it is still difficult to judge whether the NFT price can be maintained. But this

prevents some worthless NFT projects from launching. This entails a greater responsibility for project designers, who have to deal with, the consequences of not having a source of funds during the refund waiting period. ERC-721R seems to be beneficial for the development of the entire industry, but it still depends on the willingness of adoption by the project designers themselves. At present, three NFT projects have adopted this standard, namely CryptoFighters, Exodia, and Curious Addys Trading Club.

(2) **Pseudo-random allocation of rare NFTs**

How to distribute rare NFTs to minters more fairly is ERC-721R by erc721r.org's aim. It is the exact opposite of the existing NFT minting method by randomly minting tokenIDs and deterministically assigning metadata. The random assignment of tokenIDs, which is actually pseudo-random, sets an initial value based on the timestamp of the minted block. It uses the Fisher-Yates method to select an available tokenID based on a set of numbers and indexes.

This fairness from the pseudo-random assignment method can only be broken if the buyer colludes with the consensus nodes in the blockchain and sets the block's timestamp in advance. However, the cost for doing so is high and it is difficult to achieve. Therefore, even though ERC-721R uses pseudo-random assignment of tokenIDs, it can effectively ensure the fair launch of rare NFTs. Nevertheless, the method of extracting the block hash value and traversing the tokenID is very gas-consuming and not friendly to users.

```
keccak256(
    abi.encode(
        mintTargetAddress,
        tx.gasprice,
        block.number,
        block.timestamp,
        block.difficulty,
        blockhash(block.number - 1),
        address(this),
        updatedNumAvailableTokens
    )
);
```

Graph.4 Blockhash code

The value of the setting standards lies in unifying the basic attributes of NFT products, and to better facilitate developers to focus on the NFT content. The above proposed improvements to the ERC-721 standard offer some solutions to specific problems. There are also standards launched according to different

application scenarios, such as ERC1155. Under this standard, one NFT can issue multiple copies. This is more commonly used in GameFi or IP authorization. Careful selection of different NFT standards can create more value for the NFT itself. On the other hand, proposing more innovative standards can lead to the development of the entire industry. It may be a good direction for the NFT industry to re-invent itself.

Reference

1. https://www.azuki.com/erc721a
2. https://github.com/erc721r/ERC721R
3. https://docs.openzeppelin.com/contracts/3.x/erc721
4. https://erc721r.org/