NFTs: Evaluation, Opportunities and Challenges

Presented by Throne Labs, May 2021

Abstract

The Non-Fungible Token (NFT) market has been growing exponentially in recent years. The concept of NFT originally comes from a token standard of Ethereum, aiming to distinguish each token with distinguishable signs. This type of token can be bound with virtual/digital properties as their unique identifications. With NFTs, all marked properties can be freely traded with customized values according to their ages, rarity, liquidity, etc. It has greatly stimulated the prosperity of the decentralized application (DApp) market. At the time of writing (May 2021), the total money used on completed NFT sales has reached 34,530,649.86 USD. The thousandfold return on its increasing market draws huge attention worldwide. However, the development of the NFT ecosystem is still in its early stage, and the technologies of NFTs are pre-mature. Newcomers may get lost in their frenetic evolution due to the lack of systematic summaries. In this technical report, we explore the NFT ecosystems in several aspects. We start with an overview of state-of-the-art NFT solutions, then provide their technical components, protocols, standards, and desired proprieties. Afterwards, we give a security evolution, with discussions on the perspectives of their design models, opportunities and challenges. To the best of our knowledge, this is the first systematic study on the current NFT ecosystems.

1. Introduction

Non-Fungible Token (NFT) is a type of cryptocurrency that is derived by the smart contracts of Ethereum. NFT was firstly proposed in Ethereum Improvement Proposals (EIP)-721 and further developed in EIP-1155. NFT differs from classical cryptocurrencies such as Bitcoin in their intrinsic features. Bitcoin is a standard coin in which all the coins aren equivalent and indistinguishable. In contrast, NFT is unique which cannot be exchanged like-for-like (equivalently, non-fungible), making it suitable for identifying something or someone in a unique way. To be specific, by using NFTs on smart contracts (in Ethereum), a creator can easily prove the existence and ownership of digital assets in the form of videos, images, arts, event tickets, etc. Furthermore, the creator can also earn royalties each time of a successful trade on any NFT market or by peer-to-peer exchanging. Full-history tradability, deep liquidity, and convenient interoperability enable NFT to be- come a promising intellectual property (IP)-protection solution. Although, in essence, NFTs represent little more than code, but the codes to a buyer have ascribed value when considering its comparative scarcity as a digital object. It well secures selling prices of these IP-related products that may have seemed unthinkable for non-fungible virtual assets.

In recent years, NFTs have garnered remarkable attention from both the industrial and scientific communities. It was reported that the 24-hour trading volume on average of the NFT market is 4, 592, 146, 914 USD1 , while the 24-hour trad- ing volume of the entire cryptocurrency market is 341,017,001,809 USD. The liquidity of NFT-related solutions has accounted for 1.3% of the entire cryptocurrency market in such a short period (5 months). Early investors obtain thousandfold returns by selling unique digital collectibles. At the time of writing (May 2021), the NFTs-related market has significantly increased compared to one year ago (January 2020). Specifically, the total number of sales is 25,729 and their total amounts spent on completed sales reach 34,530,649.86 USD2. In particular, the total number of primary-market sales occupies 17,140, while the number of secondary sales (user-to-user) is 8, 589. Correspondingly, the total USD used on primary market sales is 8, 816, 531.10. Besides, the active market wallets achieve 12,836, which is still increasing at a high speed as time goes. Surprisingly, the sale of NFTs was estimated at 12 million (December 2020) but exploded to 340 million within just two months (February 2021). Such

skyrocketing development makes NFT become a craze, or even be described by some as the future of digital assets.

Besides the above data, people have expressed interest in various types of NFTs. They participate in NFT-related games or trades with enthusiasm. CryptoPunks, one of the first NFT on Ethereum, has created more than 10, 000 collectible punks (6039 males and 3840 females) and further promoted the ERC-721 standard to become popular. CryptoKitties officially put NFTs on notice, and hit the market in 2017 with the gamification of the breeding mechanics. Participants fiercely competed at high prices to auction the rare cats, and the highest price reaches more than 999 ETH3 (equally 3M USD). Another outstanding instance is NBA Top Shot [44], which is an NFT trading platform used to buy/sell digital short videos of NBA moments. Thousands of NBA fans from around worldwide have collected over 7.6 million top shot moments, building the roster of rookies, vets, and rising star players. Following projects also enjoy great success including Picasso Punks, Hashmasks, 3DPunks, unofficial punks, Chubbies, Bullrun Babes, Aavegotchi, CryptoCats, Moon Cats Rescue, NFT box, etc. There is no doubt that there is a hype cycle surrounding NFTs where most of products can be sold with high prices, some even hundreds or thousands of ETHs. Besides games and collectibles, NFTs also promote the development of art, ticketing event, value, IoT, and finance. Other types of surrounding markets play important roles as well to provide instant information and secure environments like statistic websites, DappRadar, NFT bank, DefiPulse, Coingecko), to trading marketplaces such as Throne Market, Opensea, SuperRare, Nifty Gateway, Rarible, and Zora.

Despite NFTs have a tremendous potential impact on the current decentralized markets and future business opportunities, the NFT technologies are still in the very early stage. Some potential challenges are required to be carefully tack- led, while some promising opportunities should be highlighted. Further, even though much literature on NFTs, from blogs, wikis, forum posts, codes and other sources, are available to the public, a systematic study is absent. This paper aims to draw attention to these questions insofar as observed and focus on summarising current NFT solutions. We provide a detailed analysis of its core components, technology roadmap status, opportunities and challenges. The contributions are provided as follows.

- Firstly, we abstract the design models of current NFT solutions. Specifically, we identify the core technical components that are used to construct NFTs. Then, we present their protocols, standards and targeted properties.

- Secondly, we give a security evaluation of current NFT systems. We adopt the STRIDE threat and risk evaluation [106] to investigate potential security issues. Based on that, we also discuss the corresponding defense measures for the issues.

- Thirdly, we explore some future opportunities of NFTs in many fields. Applying NFTs to real scenarios will boost a wide range of new applications. We give a set of practical instances (projects) leveraging NFTs with great success or prosperous markets.

- Finally, we highlight a series of open challenges in NFT ecosystems. Blockchain- based NFT systems still confront unavoidable problems like privacy issues, data inaccessibility, etc. We outline open challenges existed in state-of-the- art NFT solutions.

The rest part of this work is organized as follows. Section 2 provides the technical components used to build NFTs. Section 3 presents the protocols and standards. Based on that, Section 4 gives our security evaluation. Section 5 discusses the future opportunities, while Section 6 outlines the open challenges. Finally, Section 7 concludes this work. Appendix A gives our version updates. Appendix B and Appendix C provide NFT collectible ranking and an overview of existing NFT projects, respectively. Appendix D presents a detailed instance analysis.

2. Technical Components

In this part, we show technical components related to the NFT's activities. These components lay the building foundations of a fully functional NFT scheme.

Blockchain. Blockchain was originally proposed by Nakamoto, where Bitcoin uses the proof of work (PoW) algorithm to reach an agreement on transaction data in a decentralized network. Blockchain is defined as a distributed and attached-only database that maintains a list of data records linked and protected using cryptographic protocols. Blockchain provides a solution to the long-standing Byzantine problem, which has been agreed upon with a large network of untrusted participants. Once the shared data on the blockchain is confirmed in most distributed nodes, it becomes immutable be- cause any changes in the stored data will invalidate all subsequent data. The most prevailing blockchain platform used in NFT schemes is Ethereum, providing a secure environment for executing the smart contracts. In addition, several solutions drop their customized chain-engines or blockchain platforms to support their specialized applications, and some of them are Flow, EOS, Hyperledger, and Fast Box.

Smart Contract. Smart contracts were originally introduced by Szabo, aiming to accelerate, verify or execute digital negotiation. Ethereum further developed smart contracts in the blockchain system. Blockchain-based smart contracts adopt Turing-complete scripting languages to achieve complicated functionalities and execute thorough state transition replication over consensus algorithms to realize final consistency. Smart contracts enable unfamiliar parties and decentralized participants to conduct fair exchanges without a trusted third party and further propose a unified method to build applications across a wide range of industries. The applications operating on top of smart contracts are based on state-transition mechanisms. The states that contain the instructions and parameters are shared by all the participants, thus guaranteeing transparency of the execution of these instructions. Also, the positions between states have to stay the same across distributed nodes, which is important to its consistency. Most NFT solutions rely on smart contract- based blockchain platforms to ensure their order-sensitive executions.

Address and Transaction. Blockchain address and transaction are the essential concepts in cryptocurrencies. A blockchain address is a unique identifier for a user to send and receive the assets, which is similar to a bank account when spending the assets in the bank. It consists of a fixed number of alphanumeric characters generated from a pair of public key and private key. To transfer NFTs, the owner must prove in possession of the corresponding private key and send the assets to another address(es) with a correct digital signature. This simple operation is usually performed using a cryptocurrency wallet and is represented as sending a transaction to involve smart contracts in the ERC-777 standard.

Data Encoding. Encoding is the process of converting data from one form to another. Normally, many files are often encoded into either efficient, compressed formats for saving disk space or into an uncompressed format for high quali- ty/resolution. In the mainstream blockchain systems such as Bitcoin [98] and Ethereum [119], they employ hex values to encode transaction elements such as the function names, parameters and return values. This implies that the raw NFT data must follow these rules. If one claims s/he owns the NFT-based intellectual property, s/he essentially owns the original piece of hex values signed by the creator. Others can freely copy the raw data, but they cannot claim ownership of the property. Based on that, we can observe that the NFT-related activities (e.g. buy/sell/trade/auction) have to be processed under these four phases, similar to the basic processing procedure of smart contracts.

3. Protocols, Standards and Properties

This section presents two basic models of NFT schemes, with emphasis on their protocols, token standards and key properties.

3.1 Protocols

The establishment of NFT requires an underlying distributed ledger for records, together with exchangeable transactions for trading in the peer-to-peer network. This report primarily treats the distributed ledger as a special type of database to store NFT data. In particular, we assume that the ledger has basic security consistency, completeness, and availability characteristics. Based on that, we identify two design patterns for the NFT paradigm. The former protocol is established from top to bottom with a very simple yet classical path: building NFTs from the initiator, and then sell them to the buyer. In contrast, the later route (e.g. Loot [34], detailed analysis in Appendix D) reverses this path: setting a NFT template, and every user can create their unique ontop NFTs. We

separately provide detailed protocols of these two design patterns as below. To be noted, for both of them, they still follow a very similar workflow when executed on blockchain systems (cf. Fig.1), meaning that different designs will not change the underlying operating mechanism.

Top to Bottom. For the first design (e.g., CryptoPunks), an NFT protocol consists of another two roles: NFT owner and NFT buyer.

NFT Digitize. An NFT owner checks that the file, title, description are completely accurate. Then, they cab digitizes the raw data into a proper format.

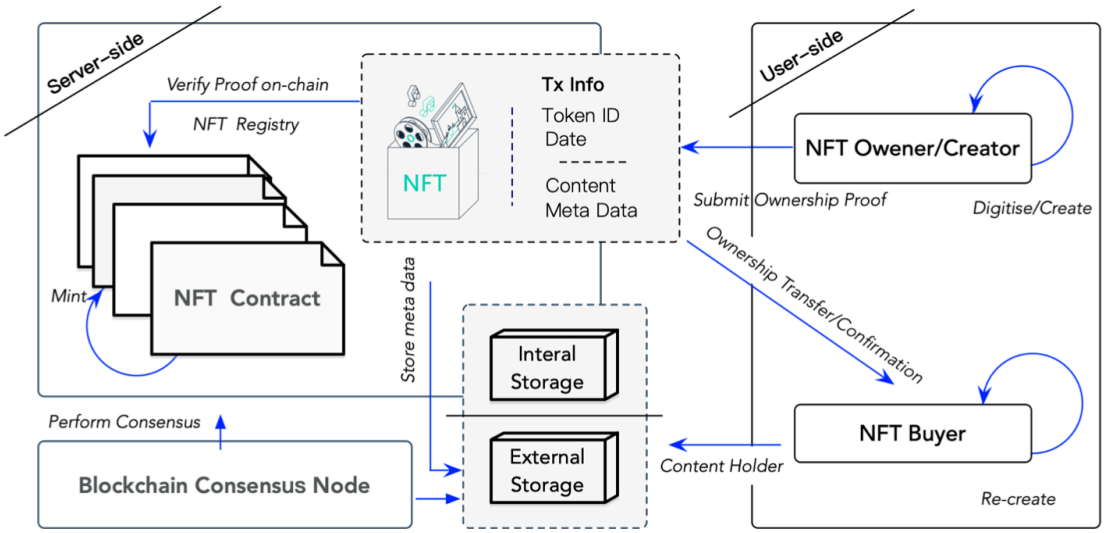

Fig. 1: Workflow of NFT System

NFT Store. An NFT owner stores the raw data into an external database outside the blockchain. Note that, a user is also allowed to store the raw data inside a blockchain, despite this operation is gas-consuming.

NFT Sign. The NFT owner signs a transaction, including the hash of NFT data, and then sends the transaction to a smart contract.

NFT Mint & Trade. After the smart contract receives the transaction with the NFT data, the minting and trading process begins. The main mechanism behind NFTs is the logic of the Token Standards that can be found in Section 3.2.

NFT Confirm. Once the transaction is confirmed, the minting process completes. By this approach, NFTs will forever link to a unique blockchain address as their persistence evidence.

Bottom to Top. For this design, the protocol consists of two roles: NFT creator and NFT buyer. In most cases, a buyer can also act as a creator because an NFT product is created based on random seeds when a buyer bids for it. This extends the functions in terms of user customization. Here, we use the superscript to highlight differences compared with the previous one.

Template Create. The project founder initiates a template via the smart contract to set up several basic rules, such as different features (character style, weapons, or accessories) in the game.

NFT Randomize. Once a buyer bids for an NFT, s/he can customize the NFT product with a set of additional features on top of basic lines. These additional features are randomly selected from a database that was predefined at the initial state.

NFT Mint&Trade. The minting and trading process starts once the corresponding smart contract is triggered.

NFT Confirm. All the procedures are conducted through smart contracts. The generated NFT will be persistently stored on-chain when the consensus procedure has been completed.

In a blockchain system, each block has a limited capacity. When the capacity in one block becomes full, other transactions will enter a future block linked to the original data block. In the end, all linked blocks have created a long-term history that remains permanent. The NFT system, in essence, is a blockchain-based application. Whenever an NFT is minted or sold, a new transaction is required to send to invoke the smart contract. After the transaction is confirmed, the NFT metadata and ownership details are added to a new block, thereby ensuring that the history of the NFT remains unchanged and the ownership is preserved.

3.2 Token Standards

In this part, we clarify token standards related to NFTs, including ERC-20, ERC-721, and ERC-1155 (see Algorithm 1). These standards have a great impact on the ongoing NFT schemes. We discuss them as follows.

Algorithm 1: NFT Standard Interfaces (with selected functions)

```
interface ERC721 {
  function ownerOf(uint256_tokenId) external view returns (address);
  function transferFrom(address_from, address_to, uint256_tokenId)
 external payable; ...
}
interface ERC1155 {
  function balanceOf(address_owner, uint256_id) external view returns
 (address);
  function balanceOfBatch(address calldata _owners, uint256 calldata
 _ids) external view returns (uint256 memory);
  function transferFrom(address_from, address_to, uint256_id, uint256
 quantity) external payable; ...
}
```

The most prevailing token standard comes from ERC-20. It introduces the concept of fungible tokens that can be issued on top of Ethereum once satisfying the requirements. The standard makes tokens the same as another one (in terms of both type and value). An arbitrary token is always equal to all the other tokens. This stimulates the hype of Initial Coin Offering (ICO) from 2015 to present. A lot of public chains and various blockchain-based DApps gain sufficient initial fundings in this way. In contrast, ERC-721 introduces a non-fungible token standard that differs from the fungible token. This type of token is unique that can be distinguished from another token. Specifically, every NFT has a uint256 variable called tokenId, and the pair of contract address and uint256 tokenId is globally unique. Further, the tokenId can be used as an input to generate special identifications such as images in the form of zombies or cartoon characters.

Another standard ERC-1155 (Multi Token Standard) extends the representation of both fungible and non-fungible tokens. It provides an interface that can represent any number of tokens. In previous standards, every tokenId in contact only contains a single type of tokens. For instance, ERC-20 makes each token type deployed in separate contracts. As well, ERC-721 deploys the group of non-fungible tokens in a single contract with the same configurations. In contrast, ERC-1155 extends the functionality of tokenId, where each of them can independently represent different configurable token types. The field may contain its customized information such as the metadata, lock-time, date, supply, or any other attributes. Here, we provide an illustration (see Fig.2) to show their structures and aforementioned differences.

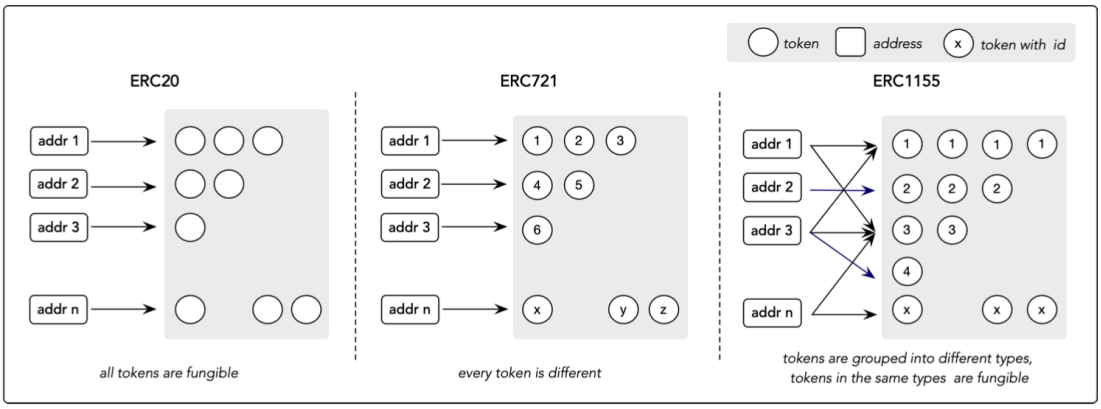

Fig. 2: NFT-related Token Standards

3.3 NFTs Desired Proprieties

NFT schemes are essentially decentralized applications, and thus enjoy the benefits/properties from their underlying public ledgers. We summarise the key properties as follows.

Verifiability. The NFT with its token metadata and its ownership can be publicly verified.

Transparent Execution. The activities of NFTs include minting, selling and purchasing are publicly accessible.

Availability. The NFT system never goes down. Alternatively, all the tokens and issued NFTs are always available to sell and buy.

Tamper-resistance. The NFT metadata and its trading records are persistently stored and cannot be manipulated once the transactions are deemed as confirmed.

Usability. Every NFT has the most up-to-date ownership information, which is user-friendly and information-clearly.

Atomicity. Trading NFTs can be completed in one atomic, consistent, iso- lated, and durable (ACID) transaction. The NFTs can run in the same shared execution state.

Tradability. Every NFTs and its corresponding products can be arbitrarily traded and exchanged.

4. Security Evaluation

An NFT system is a combination technology that consists of blockchain, storage and web application. Security evaluation on the NFT system is challenging since each component may become an attacking interface that makes the whole system really vulnerable against the attacker. Thus, we adopt the STRIDE threat and risk evaluation [106], which covers all security aspects of a system: authenticity, integrity, non repudiability, availability and access control. We investigate the potential security issues and propose some of the corresponding defense measures to address these issues (see Table 1).

Spoofing. Spoofing is the ability to impersonate another entity (for example, another person or computer) on the system, which corresponds to authenticity. When a user interacts to mint or sells NFTs, a malicious attacker may exploit authentication vulnerabilities or steal the user's private key to transfer the ownership of NFTs illegally. Thus, we recommend having a formal verification for the NFT smart contract and to use the cold wallet to prevent private key leakage.

Tampering. Tampering refers to the malicious modification of NFT data, which violates integrity. Assume that the blockchain is a robust public transaction ledger and a hash algorithm is pre-image resistance and second pre-image resistance. The metadata and ownership of NFTs cannot be maliciously modified after the transaction is confirmed. However, the data stored outside blockchain may be manipulated. Therefore, we recommend users to send both the hash data as well as the original data to the NFT buyer when trading/exchanging NFT-related properties.

Repudiation. Repudiation refers to the situation where the author of a statement cannot dispute, which is related to the security property of non-repudiability. In particular, the fact that a user sends NFT to another user cannot deny. This is guaranteed by the security of the blockchain and the un- forgeability property of a signature scheme. However, the hash data may be tampered by a malicious attacker, or the hash data may bind with an attacker's address. Thus, we believe that using a multi-signature contract can partly solve this issue since each binding must be confirmed by more than one participant.

Information Disclosure. Information leakage occurs when information is ex- posed to unauthorized users, which violates confidentiality [95]. In the NFT system, the state information and the instruction code in the smart contracts are entirely transparent, and any state and its changes are publicly accessible by any observer. Even if the user only puts the NFT hash into the blockchain, the malicious attackers can easily exploit the link-ability of the hash and transaction. Thus, we recommend the NFT developer to use privacy-preserving smart contracts instead of plain smart contracts to protect the user's privacy.

Table 1: Potential Security Issues and Corresponding Solutions of NFTs

STRIDE	Security Issues	Solutions
Spoofing *(Authenticity)*	• An attacker may exploit authentication vulnerabilities • An attacker may steal a user's private key.	• A formal verification on the smart contract. • Using the cold wallet to prevent the private key leakage.
Tampering *(Integrity)*	• The data stored outside the blockchain may be manipulated.	• Sending both the original data and hash data to the NFT buyer when trading NFTs.
Repudiation *(Non-repudiability)*	• The hash data may bind with an attacker's address.	• Using a multi-signature contract partly.
Information disclosure *(Confidentiality)*	• An attacker can easily exploit the hash and transaction to link a particular NFT buyer or seller.	• Using privacy-preserving smart contracts instead of smart contracts to protect the user's privacy.
Denial of service *(Availability)*	• The NFT data may become unavailable if the asset is stored outside the blockchain.	• Using the hybrid blockchain architecture with weak consensus algorithm.
Elevation of privilege *(Authorization)*	• A poorly designed smart contract may make NFTs lose such properties.	• A formal verification on the smart contracts.

Denial of Service (DoS). DoS attack is a type of network attack in which a malicious attacker aims to render a server unavailable to its intended users by interrupting the normal functions. DoS violates the availability and breaks down the NFT service, which can indeed be used by unauthorized users. Fortunately, the blockchain guarantees the high availability of user's operations. Legitimate users can use the required information when needed and will not lose data resources due to accidental errors. However, DoS can also be used to attack the centralized web applications or the raw data outside the blockchain, resulting in denial-of-service to NFT service. Recently, a new hybrid blockchain architecture with weak consensus algorithm was proposed, by which this architecture solves the availability issues using two algorithms.

Elevation of Privilege. Elevation of Privilege is a property that is related to the authorization. In this type of threat, an attacker may gain permissions beyond those initially granted. In the NFT system, the selling permissions are managed by a smart contract. Again, a poorly designed smart contract may make NFTs lose such properties.

5 Opportunities

This section explores the opportunities of NFTs. We discuss several typical fields which may get benefits from NFTs.

Boosting Gaming Industry. NFT has great potential in the gaming industry. There already exist some crypto games are CrytpoKitties, CryptoPunks, Meebits, Axie Infinity, Gods Unchanged, and TradeStars. A fascinating feature of such games is the "breeding" mechanism. Users can personally raise pets and spend much time breeding new off- spring. They can also purchase the limited/rare edition virtual pets, and then sell them at a high price. The extra reward attracts lots of investors to join the games, making NFTs come to prominence. Another exciting functions of the NFT are that it provides ownership records of items in the games and promotes economic marking place in the ecosystem, benefiting both developers and players. In particular, game developers who are NFT publishers of the features (e.g., weapons and skins) can earn royalties each time their items are (re-)sold on the open market. The players can obtain personal exclusivity game items. This will create a mutually beneficial business model in which both players and developers profit from the secondary NFT market. After that, blockchain communities extend NFTs to a large extent that covers various types of digital assets.

Flourishing Virtual Events. Traditional online events rely on centralized companies that provide trust and technology. Although blockchain takes over several types of activities like raising money (either by ICO/IFO/IEO/etc.), its applications are still constrained in a small range of events. NFTs greatly extend the scope of blockchain applications with the help of their additional properties (uniqueness, ownership, liquidity). This enables each individual to link to a specific event just like the patterns in our real life. We give the instance of the ticketing event. When buying tickets in a traditional event ticket market, consumers must trust the third party. Therefore, there is a risk of buying fraudulent or invalid tickets, which are possibly counterfeit or might be cancelled. The same ticket may be sold many times or obtained by extracting from ticket images posted online in an extreme case. "NFT-based ticket" represents a ticket issued by the blockchain to demonstrate entitlement to access to any event such as culture or sports. An NFT-based ticket is unique and scarce, meaning that the ticket holder cannot resell the ticket after it is sold. The blockchain-based smart contract provides a transparent ticket trading platform for the stakeholders such as the event organizer and the customer. Consumers can buy and sell the crypto ticket from the smart contract rather than rely on third parties in an efficient and reliable way.

Protecting Digital Collectibles. Digital collectibles contain a variety of types, ranging from trading cards, wines [68], digital images, videos, virtual real estate, domain names [27][64], diamonds, crypto stamps and other real/intellectual properties. We take the field of arts as an example. Firstly, artists in traditional ways have very few channels to display the works. The prices cannot reflect the true value of their works due to the absence of attention. Even worse, their published work on social networks has been charged with intermediary fees by platforms and

advertisements. NFTs transform their work into digital formats with integrated identities. Artists do not have to transfer ownership and contents to agents. This provides them impetus with lots of profits. Typical instances include Mad Dog Jones's REPLICATOR (selling with 4.1 million USD), Grimes's work (selling in total around 6 million USD [30]) and other works from great crypto-artists like Beeple / Trevor Jones. Furthermore, artists in general cases cannot receive royalties from future sales of their works. In contrast, NFTs can be programmed so that the artist receives a predetermined royalty fee each time when his digital artwork exchanges in the markets (e.g.Throne.Market, SuperRare, MakersPlace). This is an efficient way to manage and protect digital masterpieces. In addition, several platforms (e.g. Mintbase, Mintable) have even established tools to support ordinary people to create their own NFT works easily.

Inspiring the Metaverse. Metaverse is a collective virtual shared space that allows all types of digital activities. Generally, it covers a set of techniques like augmented reality and the Internet to establish the virtual world. The concept stems from the last decades and has a great progress with the rapid development of blockchain. Blockchain provides an ideal decentralized environment for the virtual online world. Participants under this blockchain-fueled alternative realities can have many types of intriguing use cases like enjoying games, displaying self-made arts, trading assets and virtual properties (arts, land parcels, names, video shots, wearables), etc. In addition, users also have opportunities to get profits from the virtual economy. They can lease the buildings (such as offices) to others to earn the bond or raise rare pets and sell them to get the rewards. Primary blockchain-empowered projects are Decentraland, Cryptovoxels, Somnium Space, MegaCryptoPolis and Sandbox. In fact, the metaverse ecosystem covers all aforementioned applications. We list it separately here simply because it is still in an early stage due to the complexity.

6. Challenges

To enable the development of the above NFT applications, a series of barriers have to be overcome as with any nascent technologies. We discuss some typical challenges from the perspectives of usability, security, governance, and extensibility, covering both the system level issues caused by blockchain-based platforms and human factors such as governs, regulation, and society.

6.1 Usability Challenges

Usability is to measure the users' effectiveness, efficiency, and satisfaction when testing a specific product/design. Most NFT schemes are built on top of Ethereum. Therefore, it is obvious that the main drawbacks of Ethereum still exist. We dis- cuss two major challenges that have direct impacts on the user experience.

Slow Confirmation. NFT-related procedures are typically conducted by sending transactions via the smart contract for reliable and transparent management (such as mint, sell, exchange). However, current NFT systems are closely coupled with their underlying blockchain platforms, which makes them suffer from low performance (Bitcoin reaches merely 7 TPS while Ethereum only 30 TPS). This results in extremely slow confirmation of NFTs. Conquering this issue requires a redesign of blockchain systems, optimization of its structure or improvement on the consensus mechanisms. Existing blockchain systems cannot fulfil such requirements.

High Gas Prices. High gas prices have become a major problem for NFT marketplaces, especially when minting the NFTs at a large scale that requires uploading the metadata to the blockchain network. Every NFT-related trans- actions are more expensive than a simple transfer transaction because smart contracts involve computational resources and storage to be processed. At the time of writing, to mine an NFT token costs over USD 60 (equivalently in around 5×102wei) 1. To complete a simple NFT trade can run between USD 60 and USD 100 for each transaction. Expensive fees caused by complex operations and high congestion greatly limit its wide adoption.

6.2 Security and Privacy Issues

The security of user data pose the first priority of systems. However, the data (stored off-chain but relates to on-chain tags) confronts the risk of losing linkage or being misused by malicious parties. We give details as follows.

NFT Data Inaccessibility. In the mainstream NFT projects [2,1,3], a cryptographic "hash" as the identifier, instead of a copy of the file, will be tagged with the token and then recorded on the blockchain to save the gas consumption. This makes the user lose confidence in the NFT because the original file might be lost or damaged. Several NFT projects integrate their system with a specialized file storage system such as IPFS [72] in which IPFS addresses allow users to find a piece of content so long as someone somewhere on the IPFS network is hosting it. Inevitably, such systems have flaws. When the users "upload" NFT metadata to IPFS nodes, there is no guarantee that their data will be replicated among all the nodes. The data may become unavailable if the asset is stored on IPFS and the only node storing it is disconnected from the network. This issue has been reported by DECRYPT.IO and CHECKMYNFT.COM. Also, an NFT might point to an erroneous file address. If that is the case, a user cannot prove that s/he actually owns the NFT. In a word, relying on an external system as the core component (storage) for an NFT system is vulnerable.

Anonymity/Privacy. In the current stage, the anonymity and privacy of NFTs are still understudied. Most NFT transactions rely on their underly- ing Ethereum platform, which only provides pseudo-anonymity rather than strict anonymity or privacy. Users can partially hide their identities if the links between their real identities and corresponding addresses are unknown by the public. Otherwise, all the activities of users under the exposed address are observable. Existing privacy-preserving solutions (e.g. homomorphic encryption), zero-knowledge proof, ring signature, multi-party computation) have not been yet applied to the NFT-related schemes due to their complicated cryptographic primitives and security assumptions. Similar to other types of blockchain-based systems, decreasing expensive computation costs becomes the key to implement privacy-promised schemes.

6.3 Governance Consideration

Similar to the situations of most cryptocurrencies, NFTs also confront the barriers like strict management from the government. On the other side, how to properly regulate this nascent technology with the corresponding market is also a challenge. We discuss two typical issues from both sides.

Legal Pitfalls. NFTs confront legal and policy issues across a wide range of areas. Potential concerned areas cover commodities, cross-border transactions, KYC (Know Your Customer) data, etc. It is important to understand the related regulatory scrutiny and litigation before moving into the NFT tracks. In some countries, such as Indian and China, the legal situation is strict for cryptocurrencies, and also for NFT sales. Exchanging, trading, selling, or buying NFTs have to overcome the difficulties of governance. Legally, users can only trade derivates on authorized exchanges such as stocks and commodities or exchange tokens with someone person-to-person. Several countries, such as Malta and France, are trying to implement suitable laws with the aim to regulate the service of digital assets. Elsewhere, issues are resolved by using existing laws. They require buyers to follow complex or even contradictory terms. Therefore, undertaking due diligence is a necessity before investing serious tokens in NFTs.

Taxable property Issues. IP-related products (including arts, books, do- main names, etc.) are treated as taxable property under the current legal framework. However, NFT-based sales stay out of this scope. Although few countries, such as the U.S. (internal revenue service, IRS), tax cryptocurrencies as property, most areas worldwide have not yet considered it. This may greatly increase the financial crimes under cover of NFT trading. The governments would love to make the sale of NFTs reliable with tax consequences. Specifically, the individual participants should have the tax liability on any capital gains that are related to NFT properties. Also, NFT-for-NFT, NFT-for-IP, and Eth-for-NFT (or vice versa) exchanges should be taxed. Furthermore, for high-profit properties, or collectibles, a higher tax bracket should be applied. Thus, NFT-related trades are suggested to seek more advice from professional tax departments after the profound discussions.

6.4 Extensibility Issues

The extensibility of NFT schemes is two-fold. The first is to stress whether a system can interact with other ecosystems. The second focuses on whether NFT systems can obtain updates when the current version is left behind.

NFT Interoperability (cross-chain). Existing NFT ecosystems are iso- lated from each other. Users once have selected one type of product can only sell/buy/trade them within the same ecosystem/network. This is due to the reason of its underlying blockchain platform. Interoperability and cross-chain communication are always the handicaps for the wide adoption of DApps. Based on the observations from, cross-chain communications can only be implemented with the help of external trusted parties. The decentralization property, in this way, has been inevitably lost to some extent. But fortunately, most of the NFT-related projects adopt Ethereum as their underlying platform. This indicates that they share a similar data structure and can exchange under the same rules.

Updatable NFTs. Transitional blockchains update their protocols through soft forks (minor modifications that are compatible forwards) and hard forks (significant modifications that may conflict with previous protocols). A formal discussion has been provided in stating the difficulties and trade- offs when applying the updates to an existing blockchain. Despite using the generic model, a new version still faces strict requirements such as tolerating specific adversarial behaviours and staying online during the update process. NFT schemes closely rely on their underlying platforms and keep consistent with them. Although the data are often stored in separate components (such as the IPFS file system), the most important logic and tokeId are still recorded on-chain. Properly updating the system with improvements will be a necessity.

7. Conclusion

Non-Fungible Token (NFT) is an emerging technology prevailing in the blockchain market. In this report, we explore the state-of-the-art NFT solutions which may re-shape the market of digital/ virtual assets stepping forward. We firstly analyze the technical components and provide the design models and properties. Then, we evaluate the security of current NFTs systems and further discuss the opportunities and potential applications that adopt the NFT concept. Finally, we outline existing research challenges that require to be solved before achieving mass-market penetration. We hope this report delivers timely analysis and summary of existing proposed solutions and projects, making it easier for newcomers to keep up with the current progress.

Please also refer to Throne Labs NFT marketplace, www.Throne.Market

References

Decentraland (mana). Project accessible: https://decentraland.org/ (2020)

Flow. Project accessible: https://www.onflow.org/ (2020)

Sandbox. Project accessible: https://www.sandbox.game/en/ (2020)

3d punks. Project Accessible: http://www.3dpunks.com/ (2021)

Aavegotchi. Project Accessible: https://aavegotchi.com/ (2021)

Alien worlds. Project Accessible: https://alienworlds.io/ (2021)

Art blocks. Project Accessible: https://artblocks.io/ (2021)

Async art. Project Accessible: https://async.art/ (2021)

Axie infinity. Project Accessible: https://axieinfinity.com/ (2021)

Beeple. Project Accessible: https://www.beeple-crap.com/ (2021)

Bored ape yacht club. Project Accessible: https://boredapeyachtclub.com/#/ (2021)

Bullrun babes. Project Accessible: https://opensea.io/collection/bullrunbabestoken (2021)

Cargo. Project Accessible: https://cargo.build/ (2021)

Chubbies. Project Accessible: https://chubbies.io/ (2021)

Coingecko website. Accessible: https://coingecko.com/en (2021)

Cometh. Project Accessible: https://www.cometh.io/ (2021)

Crypto stamp. Project Accessible: https://crypto.post.at/ (2021)

Cryptocats. Project Accessible: https://cryptocats.thetwentysix.io/ (2021)

Cryptokitties. Project Accessible: https://www.cryptokitties.co/ (2021)

Cryptopunks. Accessible: https://www.larvalabs.com/cryptopunks (2021)

Cryptoslam. Project Accessible: https://cryptoslam.io/ (2021)

Cryptovoxels. Project Accessible: https://www.cryptovoxels.com/ (2021)

Cryptowine. Project Accessible: https://grap.finance/#/ (2021)

Dappradar website. Accessible: https://dappradar.com/ (2021)

Dego. Project Accessible: https://dego.finance/ (2021)

Deipulse website. Accessible: https://defipulse.com/ (2021)

Ens domains. Project Accessible: https://app.ens.domains/ (2021)

Fast box. Project Accessible: https://www.fastbox.cc/ (2021)

Gods unchanged. Project Accessible: https://godsunchained.com/ (2021)

Grimes sold $6 million worth of digital art as nfts. News source: https://www.theverge.com/2021/3/1/22308075/grimes-nft-6-million- sales-nifty-gateway-warnymph (2021)
16

Hashmasks. Project Accessible: https://www.thehashmasks.com/ (2021)

Icecap. Project Accessible: https://icecap.diamonds/ (2021)

Known origin. Project Accessible: https://www.knownorigin.io/ (2021)

Loot contract code. https://etherscan.io/address/0xff9c1b15b16263c61d017ee9f65c50e4ae0113d7#code (2021)

Loot talk. https://loot-talk.com/ (2021)

Mad dog jones. News source: https://www.phillips.com/detail/mad-dog-jones/NY090121/1 (2021)

Makersplace. Project Accessible: https://makersplace.com/ (2021)

Meebits. Project Accessible: https://meebits.larvalabs.com/ (2021)

Megacryptopolis. Project Accessible: https://mcp3d.com/ (2021)

Mintable. Project Accessible: https://mintable.app/ (2021)

Mintbase. Project Accessible: https://www.mintbase.io/ (2021)

Moon cats rescue. Project Accessible: https://mooncatrescue.com/ (2021)

Mycryptoheroes. Project Accessible: https://www.mycryptoheroes.net/ (2021)

Nba top shot. Accessible: https://nbatopshot.com/ (2021)

Nft bank. Project Accessible: https://nftbank.ai/ (2021)

Nft box. Project Accessible: https://nftboxes.io/ (2021)

Nft diamonds. Project Accessible: https://nftdiamonds.co/ (2021)

Nifty gateway. Project Accessible: https://niftygateway.com/ (2021)

Nonfungible website. Accessible: https://NonFungible.com (2021)

Opensea platform. Accessible: https://opensea.io/ (2021)

Picasso punks. Accessible: https://opensea.io/collection/picassopunks (2021)

Polkamon. Project Accessible: https://polkamon.com/ (2021)

R planet. Project Accessible: https://rplanet.io/ (2021)

R.a.r.e art lab. Project Accessible: https://www.lagelnd.com/rare (2021)

Rarible. Project Accessible: https://rarible.com/ (2021)

Skyweaver. Project Accessible: https://www.skyweaver.net/ (2021)

Somnium space. Project Accessible: https://somniumspace.com/ (2021)

Sorare. Project Accessible: https://sorare.com/ (2021)

Superrare. Project Accessible: https://superrare.co/ (2021)

Topps mlb. Project Accessible: https://toppsmlb.com/ (2021)

Tradestars. Project Accessible: https://tradestars.app/ (2021)

Trevorjonesart. Project Accessible: https://www.trevorjonesart.com/ (2021)

Unofficial punks. Project Accessible: https://opensea.io/collection/unofficialpunks (2021)

Unstoppable domains. Accessible: https://unstoppabledomains.com/ (2021)

Viv3. Project Accessible: https://VIV3.com (2021)

Wax: Worldwide asset exchange. Accessible: https://on.wax.io/wax-io/ (2021)

Wax:worldwide asset exchange. Project Accessible: https://github.com/worldwide-asset-exchange/whitepaper (2021)

Wiv. Project Accessible: https://www.wiv.io/ (2021)

Zora. Project Accessible: https://zora.co/ (2021)

Bal, M., Ner, C.: Nftracer: a non-fungible token tracking proof-of-concept using hyperledger fabric. arXiv preprint arXiv:1905.04795 (2019)

Bano, S., Sonnino, A., Al-Bassam, M., Azouvi, S., McCorry, P., Meiklejohn, S., Danezis, G.: Sok: Consensus in the age of blockchains. In: Proceedings of the 1st ACM Conference on Advances in Financial Technologies. pp. 183–198 (2019)

Benet, J.: Ipfs-content addressed, versioned, p2p file system. arXiv preprint

arXiv:1407.3561 (2014)
17
Benson, J.: Your nfts can go missing—here's what you can do about it. https: //decrypt.co/62037/missing-or-stolen-nfts-how-to-protect (2021)

Buterin,V.,etal.:Anext-generationsmartcontractanddecentralizedapplication platform. white paper 3(37) (2014)

Cai, W., Wang, Z., et al.: Decentralized applications: The blockchain-empowered software system. IEEE Access 6, 53019–53033 (2018)

CH21: Check my nft. https://checkmynft.com/ (2021)

Chevet, S.: Blockchain technology and non-fungible tokens: Reshaping value chains in creative industries. Available at SSRN 3212662 (2018)

Chohan, U.W.: Non-fungible tokens: Blockchains, scarcity, and value. Critical Blockchain Research Initiative (CBRI) Working Papers (2021)

Ciampi, M., et al.: Updatable blockchains. In: European Symposium on Research in Computer Security. pp. 590–609. Springer (2020)

Dowling, M.M.: Fertile land: Pricing non-fungible tokens. Available at SSRN 3813522 (2021)

Fabian, V., Vitalik, B.: Eip-20: Erc-20 token standard. Accessible: https://eips .ethereum.org/EIPS/eip-20 (2015)

Fairfield, J.: Tokenized: The law of non-fungible tokens and unique digital property. Indiana Law Journal, Forthcoming (2021)

Franceschet, M., Colavizza, G., Smith, T., et al.: Crypto art: A decentralized view. Leonardo pp. 1–8 (2020)

Garay, J., Kiayias, A.: Sok: A consensus taxonomy in the blockchain era. In: Cryptographers' Track at the RSA Conference. pp. 284–318. Springer (2020)

Garay,J.,Kiayias,A.,Leonardos,N.:Thebitcoinbackboneprotocol:Analysisand applications. In: Annual International Conference on the Theory and Applications
of Cryptographic Techniques (EUROCRYPT). pp. 281–310. Springer (2015)

Garay, J., Kiayias, A., Leonardos, N.: The bitcoin backbone protocol with chains of variable difficulty. In: CRYPTO. pp. 291–323. Springer (2017)

Gervais, A., et al.: On the security and performance of proof of work blockchains. In: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Com-
munications Security. pp. 3–16. ACM (2016)

Gudgeon, L., Moreno-Sanchez, P., Roos, S., McCorry, P., Gervais, A.: Sok: Layer-two blockchain protocols. In: International Conference on Financial Cryptography and Data Security. pp. 201–226. Springer (2020)

Hong, S., Noh, Y., Park, C.: Design of extensible non-fungible token model in hyperledger fabric. In: Proceedings of the 3rd Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers. pp. 1–2 (2019)

Jacques, D., Jordi, B., Thomas, S.: Eip-777: Erc-777 token standard. Accessible: https://eips.ethereum.org/EIPS/eip-777 (2017)

Johnson, K.N.: Decentralized finance: Regulating cryptocurrency exchanges. William & Mary Law Review 62 (2021)

Lamport, L., Shostak, R., Pease, M.: The byzantine generals problem. In: Concurrency: the Works of Leslie Lamport, pp. 203–226 (2019)

Li, R., Galindo, D., Wang, Q.: Auditable credential anonymity revocation based on privacy-preserving smart contracts. In: Data Privacy Management, Cryptocurrencies and Blockchain Technology, pp. 355–371. Springer (2019)

Li, R., et al.: An accountable decryption system based on privacy-preserving smart contracts. In: International Conference on Information Security. pp. 372–
390. Springer (2020)

Menezes, A.J., Van Oorschot, P.C., Vanstone, S.A.: Handbook of applied cryp-

tography. CRC press (2018)
18
Moore, D., Voelker, G., Savage, S.: Inferring internet denial-of-service activity. ACM Trans. Comput. Syst. 24, 115–139 (2006)

Musan, D.I., William, J., Gervais, A.: Nft. finance leveraging non-fungible tokens (2020)

Nakamoto,S.:Bitcoin:Apeer-to-peerelectroniccashsystem.Tech.rep.,Manubot (2019)

Noether, S.: Ring signature confidential transactions for monero. IACR Cryptol. ePrint Arch. 2015, 1098 (2015)

Omar, A.S., Basir, O.: Capability-based non-fungible tokens approach for a de- centralized aaa framework in iot. In: Blockchain Cybersecurity, Trust and Privacy, pp. 7–31. Springer (2020)

Raman, R.K., et al.: Trusted multi-party computation and verifiable simulations: A scalable blockchain approach. arXiv preprint arXiv:1809.08438 (2018)

Raval, S.: Decentralized applications: harnessing Bitcoin's blockchain technology. " O'Reilly Media, Inc." (2016)

Regner, F., Urbach, N., Schweizer, A.: Nfts in practice–non-fungible tokens as core component of a blockchain-based event ticketing application (2019)

Rogaway, P., Shrimpton, T.: Cryptographic hash-function basics: Definitions, im- plications, and separations for preimage resistance, second-preimage resistance, and collision resistance. In: FSE. pp. 371–388. Springer (2004)

Shirole, M., Darisi, M., Bhirud, S.: Cryptocurrency token: An overview. IC-BCT 2019 pp. 133–140 (2020)

Shostack, A.: Experiences threat modeling at microsoft. MODSEC@ MoDELS 2008 (2008)

Szabo, N.: Smart contracts: building blocks for digital markets. EXTROPY: The Journal of Transhumanist Thought,(16) 18(2) (1996)

Trautman, L.J.: Virtual art and non-fungible tokens. Available at SSRN 3814087 (2021)

Valdeolmillos, D., et al.: Blockchain technology: a review of the current challenges of cryptocurrency. In: International Congress on Blockchain and Applications. pp. 153–160. Springer (2019)

Wang, G., et al.: Sok: Sharding on blockchain. In: Proceedings of the 1st ACM Conference on Advances in Financial Technologies. pp. 41–61 (2019)

Wang, Q., Li, R.: A weak consensus algorithm and its application to high- performance blockchain. In: IEEE INFOCOM 2021-IEEE Conference on Computer Communications (INFOCOM). IEEE (2021)

Wang, Q., Qin, B., Hu, J., Xiao, F.: Preserving transaction privacy in bitcoin. Future Generation Computer Systems 107, 793–804 (2020)

Wang, Q., Yu, J., Chen, S., Xiang, Y.: Sok: Diving into dag-based blockchain systems. arXiv preprint arXiv:2012.06128 (2020)

Wang, Y., Kogan, A.: Designing confidentiality-preserving blockchain-based transaction processing systems. International Journal of Accounting Information Systems 30, 1–18 (2018)

William, E., Dieter, S., Jacob, E., Nastassia, S.: Eip-721: Erc-721 non-fungible token standard. Accessible: https://eips.ethereum.org/EIPS/eip-721 (2018)

William, E., Dieter, S., Jacob, E., Nastassia, S.: Erc-721 non-fungible token stan- dard. Ethereum Improvement Protocol, EIP-721, Accessible: https://eips.eth ereum.org/EIPS/eip-721. (2018)

Witek, R., Andrew, C., Philippe, C., James, T., Eric, B., Ronan, S.: Eip-1155: Erc-1155 multi token standard. Ethereum Improvement Protocol, EIP-1155, Ac- cessible: https://eips.ethereum.org/EIPS/eip-1155. (2018)
19

Witek, R., et al.: Eip-1155: Erc-1155 multi token standard. Accessible: https: //eips.ethereum.org/EIPS/eip-1155 (2018)

Wood, G., et al.: Ethereum: A secure decentralised generalised transaction ledger. Ethereum project yellow paper 151(2014), 1–32 (2014)

Zamyatin, A., et al.: Sok: communication across distributed ledgers. (2019)

Zhou, J., Gollman, D.: A fair non-repudiation protocol. In: Proceedings 1996
IEEE Symposium on Security and Privacy. pp. 55–61. IEEE (1996)