JOURNAL PUNJAB ACADEMY OF SCIENCES (Peer Reviewed Open Access Journal)
JPAS, 22: 33-48 (January-December, 2022)
Available online at www.jpas.in
ISSN 2229-7014 (P)

Non-Fungible Token (NFT): Survey, Analysis, Benefits, and Provocation

Sahil Bansal[1] . Amrit Kaur Bhullar[2]

[1,2]*Department of Electronics & Communication Engineering Punjabi University, Patiala, Punjab, India,* sahilbansal152001@gmail.com[1] amritbhullar@pbi.ac.in[2].

ABSTRACT

The Non-Fungible Token (NFT) marketplace has been growing rapidly in recent years, inspired by the Ethereum token. At the time of writing, the total cash used on finished NFT income has reached 34,530,649.86 USD. However, the improvement of the NFT environment remains in its early stage, and the technology of NFT is premature. This technical report provides a top-level view of contemporary NFT solutions, technical components, protocols, standards, and favored proprieties, as well as a safety evolution.

Keywords: NFT,· Blockchain , Smart Contract , DApp· Metaverse

INTRODUCTION

A non-Fungible Token (NFT) is a kind of cryptocurrency [1] that is derived with the help of using the smart contracts of Ethereum [99]. NFT changed into first proposed in Ethereum Improvement Proposals (EIP)-721 [96] and similarly developed in EIP-1155 [97]. NFT differs from classical cryptocurrencies [86] consisting of Bitcoin of their intrinsic features. Bitcoin is a preferred coin in which all the cash is equal and indistinguishable. In contrast, NFT is precise and can't be exchanged like-for-like (equivalently, non-fungible), making it appropriate for figuring out something or a person in a unique way. To be specific, with the help of using the use of NFTs on smart contracts (in Ethereum [99]), a writer can effortlessly show the lifestyles and possession of virtual belongings withinside the shape of videos, images, arts [66], occasion tickets [84], etc. Furthermore, the writer also can earn royalties every time a hit alternates on any NFT marketplace or with the help of using the peer-to-peer exchange. Full-records tradability, deep liquidity, and handy interoperability permit NFT to grow to be a promising highbrow property (IP)-safety solution. Although, in essence, NFTs constitute little greater than code, however, the codes to a consumer have recognized price while thinking about its comparative shortage as a virtual object. It nicely secures promoting fees of that IP-associated merchandise that could have been regarded as unimaginable for non-fungible digital belongings.

NFTs are digital assets that represent real-world objects such as art, music, in-game items, and videos. They are often bought and sold online using cryptocurrencies and are usually encoded in the same underlying software as many cryptocurrencies. The NFT has been around since 2014 and is now notorious as it is becoming an increasingly popular way to buy and sell digital art. Since March 2022, a staggering $ 180 million has been spent on NFTs. The NFT is also generally unique, or at least a very limited edition, and has a unique identification code. "In essence, NFTs create digital rarity," said Arry Yu, chair of the Cascadia Blockchain Council of the Washington Technology Industry Association and executive director of Yellow Umbrella

Ventures. This is in stark contrast to most digital works, which are virtually endlessly available. If the supply cut is to increase the value of a particular asset, assume demand. However, many NFTs have survived in one way or another, at least initially, such as iconic music videos from NBA games and certified digital art versions. was popular on Instagram. It's digital work. For example, acclaimed digital artist Mike Winkelmann, better known by his nickname "Beeple," [8] aggregated 5,000 images a day to create perhaps the most famous NFT,

"EVERYDAYS: The First 5000 Days" (see Figure 1). It set a sales record for Christie`s. 69.3 million dollars.

Fig. 1: - Everydays: The First 5000 Days

Anyone can view individual images or entire collages online for free. So why are people willing to pay millions for what they can scan or download? NFT allows the buyer to own the original item. Plus, it includes a built-in certificate that acts as proof of ownership. Collectors appreciate these "digital bragging rights" almost more than the items themselves.

In recent years, NFT has attracted considerable interest from the commercial and medical communities. It can be suggested that the 24-hour buy and sell range on the NFT market is ($4,592,146,914)1 while the full crypto market 24-hour buy and sell range is at $341,017,001,809. The liquidity of NFT-related responses accounted for 1.3% of the entire crypto market in a short period (five months). First-time buyers receive thousands of times more returns through advertising-specific virtual collections. At the time of writing (March 2022), the NFT-related market has improved significantly compared to 2 years ago. before (January 2020). Specifically, their total diversified income is 60,678, and their combined amount spent on finished income comes in at ($54,530,649,86)2. The total diversified income of the number one market accounted for 17,140, while the diversified secondary income (from users to users) was 9,784,816, 531.10. Additionally, the market's dynamic portfolio sits at 12,836, continuing to grow at an exaggerated rate over time. Surprisingly NFT sales increased to 12 million (December 2020) but exploded to 340 million in just a few months (February 2021). Such a metric improvement makes NFT a craze or could be defined by some as the future of virtual assets.

The rest of this work is structured as follows: Section 2 provides the technical components used to create the NFT. Section 3 introduces protocols and standards. Based on this, Section 4 reflects our safety assessment. Section 5 describes future opportunities and Section 6 outlines future challenges. Finally, Section 7 finishes this work. Appendix A and Appendix B provide a comprehensive NFT ranking and an overview of existing NFT projects. Appendix C contains a detailed instance analysis. Appendix D tells the security of NFTs according to time with 2 different blockchains.

This part shows the technical components related to NFT activities. These components form the basis for building a fully functional NFT system.

Blockchain.

The blockchain was originally proposed by Nakamoto [80], where Bitcoin uses a proof-of-

work (PoW) [70] algorithm to reach an agreement on transaction data in a decentralized network. Blockchain is defined as a distributed, constrained database that maintains a linked list of data records and is protected using cryptographic protocols [69]. Blockchain provides a solution to the age-old Complicated problem [75], which has been agreed upon with a large network of unreliable participants. Once the data shared on the blockchain is confirmed in most of the distributed nodes, it becomes immutable as any modification to the stored data will invalidate all subsequent data. The most widely used blockchain platform in NFT schemes is Ethereum [2], which provides a secure environment for the execution of smart contracts. Additionally, several solutions are leaving their custom blockchain tools or blockchain platforms to support their specialized applications, and some of them are Flow [2], EOS [53], Hyperledger [72][56], and Fast Box [21][91].

Smart Contract.

Smart contracts were originally introduced by Szabo [88], aiming to accelerate, verify or execute digital negotiation. Ethereum [2] further developed smart contracts in the blockchain system [67][57]. 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 statements and parameters are shared by all participants, thus ensuring the transparency of the execution of these statements. Furthermore, the position between states must be preserved across distributed nodes, which is important for its consistency. Most blockchain-based NFT solutions rely on smart contracts to ensure their order-sensitive execution.

Decentralized Application.

A decentralized application (DApp) is a type of distributed open-source software application that runs on a peer-to-peer (P2P) blockchain network rather than on a single computer. DApps look like other software applications supported on a website or mobile device but are supported via P2P. The decentralized nature of a DApp means that once a developer has released the code base for a DApp, others can develop it. This application does not have the control of a single agency. A DApp is developed to create many types of applications, including those for decentralized finance, web browsing, gaming, and social media. The DApp is built on a decentralized network backed by a blockchain- distributed ledger. Using blockchain allows a DApp to process data through distributed networks and execute transactions. DApps are also often built using the Ethereum platform. Distributed ledger technologies like the Ethereum blockchain have helped popularize DApps. The main advantage of DApps is that they are always accessible and there is no point in failure (see figure 2).

1 Data source from Coingecko (May 2022) https://www.coingecko.com/en /nft
2 Data captured from https://www.nonfungible.com/market/history

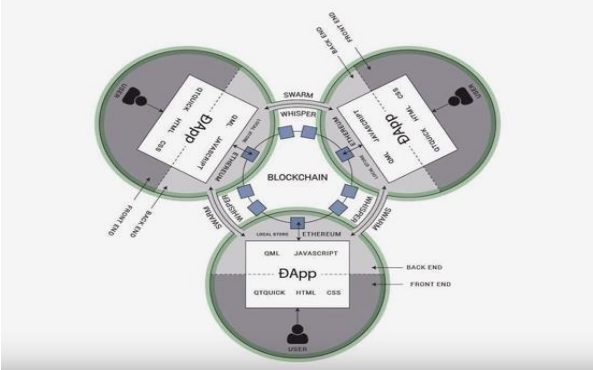

Fig. 2: -Workflow of DApp

Address and Transaction.

Blockchain addresses and transactions are core concepts of cryptocurrencies. A blockchain address is a unique identifier for users to send and receive assets, similar to a bank account when spending assets in a bank. It consists of a fixed number of alphanumeric characters generated from a pair of public and private keys. To transfer NFTs, the owner must prove that he has the corresponding private key and send the content to one or more other addresses with the correct digital signature. This simple operation is usually performed using a cryptocurrency wallet and is represented as sending a transaction involving smart contracts according to the ERC777 [73] standard.

Data Encoding.

Encoding is the system of changing information from one shape to another. Normally, many documents are regularly encoded into efficient, compressed codecs for saving disk space or into an uncompressed layout for excessive quality/resolution. In the mainstream blockchain structures including Bitcoin [80] and Ethereum [99], they appoint hex values to encode transaction factors including the character names, parameters, and return values. This means that the raw NFT information ought to observe those rules. If one claims he/she owns the NFT-primarily based intellectual property, he/she owns the unique piece of hex values signed via way of means of the creator. Others can freely reproduce the raw information; however, they cannot declare possession of the property. Based on that, we will study that the NFT-associated activities (e.g., buy/sell/trade/auction) ought to be processed underneath those 4 phases, much like the primary processing system of clever contracts.

Protocols, Standards, and Properties

This section introduces two fundamental kinds of NFT systems, emphasizing their protocols, token standards, and essential attributes.

Protocols

Setting up the NFT requires an underlying distributed ledger for records, as well as exchangeable transactions for peer-to-peer transactions. This report mainly considers the distributed ledger as a special type of database for storing NFT data. We assume that the ledger has the basic characteristics of security, completeness, and availability. Based on this, we define two design patterns for the NFT model. The old protocol was established from the top with a very simple but classic path: build NFTs from the initiator, then sell them to buyers. In contrast, the next route (e.g., Loot [27], detailed analysis in Appendix D) reverses this path: define an NFT model, and each user can create their own on the best NFT. We provide separately detailed protocols for these two designs as below. Note, for they still follow a very similar workflow when running on blockchain systems (see Figure 3), which means that different designs will not change the underlying mechanism of operation

From top to bottom.

For the original design (such as CryptoPunks [16]), the NFT protocol consisted of two roles: NFT holder and NFT buyer.

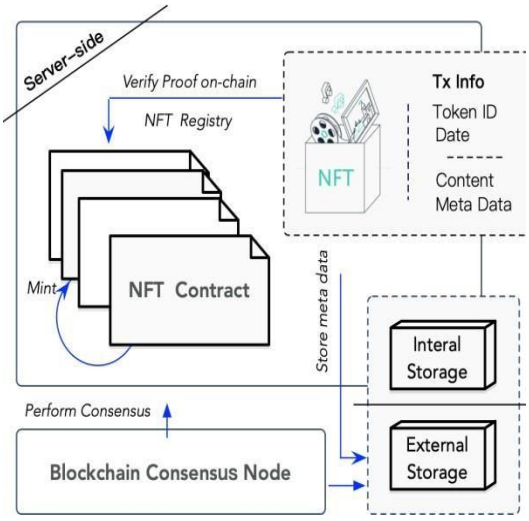

Fig. 3-: Workflow of NFT System

NFT Digitize. The NFT owner verifies that the file, title, and description are completely correct. It then digitizes the raw data into a suitable format.

NFT Store. NFT holders store raw data in an external database outside of the blockchain. Note that it is also allowed to store raw data inside a blockchain, although this operation costs a gas fee.

NFT Sign.NFT holders sign a transaction, including hashing NFT data, and then send the transaction to a smart contract.

NFT Mint & Trade. Once the smart contract receives the NFT knowledge relationships, the minting and marketing will begin. The most important mechanism behind NFT is the token standard logic described in Section 3.2.

NFT Confirm. Once the transaction is confirmed, the minting process ends. By taking this approach, NFTs will always be tied to a unique blockchain address as proof of persistence.

Bottom to High. For this style (e.g., Loot [27]), the protocol includes 2 roles: NFT creator and NFT buyer. In maximum cases, the buyer may also act as a writer due to an NFT product being shaped and supported by random seeds as soon as the emptor bid for it. This extends the capabilities in phrases of person customization. Here, we tend to use the superscript $*$ to focus on variations compared with the previous one.

Template Create*. The project founder initiates a model through a smart contract to implement some basic rules, such as different features (character style, weapon, or accessory) in the game.

NFT Randomize. After a buyer places a bid on the NFT, they can customize the NFT product with a set of extras at the top of the baseline. These extras are randomly selected from a predefined database in the initial state.

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

NFT Confirm. The minting and trading process starts once the corresponding smart contract is triggered.

In a blockchain system, each block has a limited capacity. When the capacity of a block becomes full, other transactions will enter a future block associated with the original data block. In the end, all the linked blocks created a long story that lasts forever. In essence, the NFT system is a blockchain-based application. Each time an NFT is minted or sold, a new transaction must be sent to invoke the smart contract. Once the transaction is confirmed, the NFT metadata

and ownership details are added to a new block, ensuring that the history of the NFT is unchanged and ownership is preserved.

Token Standards

In this section, we clarify NFT-related token standards, including ERC20 [64], ERC721 [95], and ERC1155 [98] (see Algorithm 1). These standards have a significant impact on ongoing NFT programs. 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 balance Of(address owner,
uint256 id) external view returns
(address); function balanceOfBatch(address
call data owners, uint256 call data
ids) external view returns (uint256 memory);
function transfer From(address from, address
to, uint256 id, uint256
quantity) external payable; ...
}

The most popular token standard comes from ERC20 [64]. It introduces the concept of fungible tokens that can be issued on Ethereum as they fulfill the requirements. The standard makes the tokens identical (in terms of type and value). An arbitrary token is always equal to all other tokens. This drives the initial coin offering (ICO) from 2015 to the present. Various public channels and blockchain-based DApps [61][83] obtained sufficient initial capital this way. In contrast, ERC721 [95] introduces a non-fungible token standard, which is different from a fungible token. This type of token is unique and can be distinguished from other tokens. Specifically, each NFT has a uint256 variable called TokenId, and the contract address pair and uint256 TokenId are globally unique. In addition, TokenId can be used as input to generate special identifiers such as images in the form of zombies or cartoon characters.

Another standard, ERC1155 (multi-token standard) [98], extends the representation of both fungible and non-fungible tokens. It provides an interface that can represent any number of tokens. In the previous standard, each contact TokenId contained only a single type of token. For example, ERC20 provides each token type in a separate contract. ERC721 also expands a group of non-fungible tokens in a single contract with the same configuration. In contrast, the ERC1155 can extend the functionality of TokenId, each independently representing a different configurable token type. This field can contain custom information such as metadata, lock time, date, supply, and other attributes. Here we provide a diagram (see Figure 4) to show their structure and the differences above.

STRIDE	Security Issues	Solutions
Spoofing (Authenticity)	An attacker may exploit authentication vulnerabilities. An attacker may steal a user's private key.	Formal verification of the smart contract. Using the cold wallet to prevent 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 contractpartly.
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	Using the hybrid blockchain architecture with a weak consensus algorithm.

	blockchain.	
Elevation of Privilege (Authorization)	A poorly designed smart contract may make NFTs lose such properties.	Formal verification of the smart contracts.

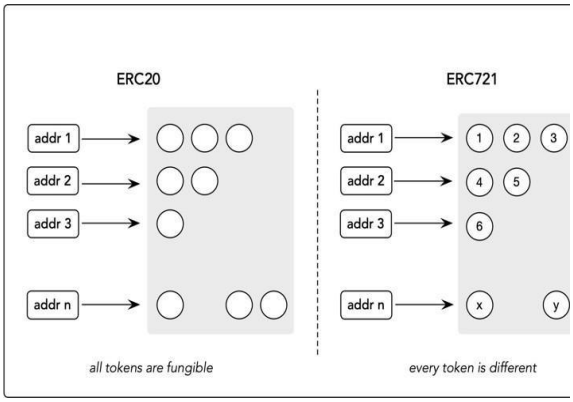

Fig. 4 NFT-related Token Standards

Desired Properties of NFTs

NFT schemes are decentralized applications [60] and thus enjoy the benefits/properties from their underlying public ledgers. The important key properties are summarized as follows.

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

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

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

Tamper-resistance. The NFT metadata and its transaction records are stored persistently and cannot be manipulated once a transaction is held and confirmed.

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

Atomicity. NFT transactions can be executed in an Atomic, Consistent, Isolated, and Durable (ACID) transaction. NFTs can run in the same shared execution state.

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

4 Security Evaluation

The NFT system is a combined technology that includes blockchain, storage, and web applications. Evaluating security on an NFT system is difficult because each component can become an attacking interface making the entire system truly vulnerable to an attacker. Therefore, we apply STRIDE risk and threat assessment [87], which covers all security aspects of the system: authenticity, integrity, reputation lessness, availability, and access control. We investigate potential security issues and recommend some corresponding defenses to address them (see Table 1)

Spoofing. Spoofing is the ability to impersonate another entity (for example, another person or a computer) on the system, corresponding to authenticity. When users interact with mint or sell NFTs, a malicious attacker can exploit authentication vulnerabilities or steal users' private keys to illegally transfer ownership of NFTs. Therefore, we recommend you formally verify the NFT smart contract and use cold wallets to avoid private key leakage.

Tampering. Tampering refers to the malicious modification of NFT data, a violation of integrity. Assume the blockchain is a strong public ledger of transactions [68][69] and the hashing algorithm is a second pre-image resistor [85]. NFT metadata and ownership cannot be maliciously altered after transaction confirmation. However, data stored outside of the blockchain can be manipulated. Therefore, it is recommended that users submit both hash data as well as original data to NFT buyers when trading/exchanging NFT-related properties.

Repudiation. Repudiation refers to the situation where the author of a statement cannot dispute [101], which is related to the security property of non-cancellation [78]. In particular,

the fact that one user sends NFT to another is undeniable. This is ensured by the security of the blockchain and the tamper-proof property of a signature scheme. However, the hash data can be altered by a malicious attacker, or the hash data can be tied to the attacker's address. Therefore, we believe that using a multi-signature contract can partially solve this problem because each link must be validated by more than one participant.

Information Disclosure. Information leakage occurs when information is exposed to unauthorized users, violating confidentiality. In the NFT system, the state information and instruction code in the smart contract is completely transparent and any state and its changes are publicly accessible by any observer. Even if a user just puts the NFT hash on the blockchain, malicious

attackers can easily exploit the link-ability of the hash and the transaction. Therefore, we recommend NFT developers use privacy-preserving smart contracts [76][77] instead of simple smart contracts to protect user privacy.

Denial of Service (DoS). A DoS attack [79] is a type of cyber- attack in which a malicious attacker aims to make a server unavailable to its intended users by disrupting normal functions. DoS violates the availability and breaks the NFT service, which can be used by unauthorized users. Fortunately, blockchain ensures high availability for user activities.

Legitimate users can use necessary information as needed and will not lose data resources due to accidental errors. However, DoS can also be used to attack centralized web applications or raw data outside of the blockchain, resulting in a denial of NFT service. Recently, a new hybrid blockchain architecture with a weak consensus algorithm has been proposed [91], whereby this architecture solves the availability problems by using two algorithms.

Elevation of Privilege. Privilege elevation [87] is a permission- related attribute. In this type of threat, an attacker can obtain permissions beyond those originally granted. In the NFT system, the sales authorization is managed by a smart contract. Again, a poorly designed smart contract can cause the NFT to lose such properties.

Opportunities

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

Boosting the Game Industry. NFT has great potential in the gaming industry. Crypto games like CrytpoKitties, Cryptocats [37], CryptoPunks [16], Meebits [31], Axie Infinity [39], Gods Unchanged [22], and TradeStars [49] are available now. An attractive feature of these games is the "breeding" mechanic. Users can manually raise pets and spend a lot of time raising new children. They can also buy rare/limited edition virtual pets and then resell them for a premium price. The side bonus attracts more investors to the game, which makes NFT stand out. Another interesting function of NFT is that it provides ownership records of in-game items and promotes economic marking place in the ecosystem, benefiting both developers and players. Game developers who are NFT publishers of features (e.g., weapons and skins) can earn royalties each time their items are (re)sold on the open market. Players can receive individual exclusive game items. This will create a win-win business model in which 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 occasions depend on centralized businesses that offer acceptance as true with technology. Although blockchain takes over numerous styles of sports like elevating money (both through ICO/IFO/IEO/etc.), its packages are

nevertheless restrained on a small variety of occasions. NFTs substantially make bigger the scope of blockchain packages with the assistance of their extra properties (uniqueness, ownership, liquidity). This allows every character to hyperlink to a particular occasion like the styles in our actual life. We supply an example of the ticketing occasion. When shopping for tickets in a conventional occasion ticket market, clients need to accept it as true with the third party. Therefore, there may be a chance of purchasing fraudulent or invalid tickets, which can be probably counterfeit or are probably cancelled. The identical ticket can be bought normally or received by extracting from ticket photographs published online in an excessive case. "NFT-primarily based ticket" represents a ticket issued through the blockchain to illustrate entitlement to get admission to any occasion inclusive of lifestyle or sports. An NFT- primarily based ticket is totally precise and scarce, which means that the ticket holder can't resell the tickets after it's far bought. The blockchain-primarily based clever agreement affords an obvious ticket-buying and selling platform for the stakeholders inclusive of the occasion organizer and the customer. Consumers can purchase and promote crypto tickets from the clever agreement in preference to depend on 0.33 events in a green and dependable way.

Protecting Digital Collectibles. Digital Collections include a wide range of categories ranging from trading cards, wines, digital images, videos, virtual real estate, domains, diamonds, crypto stamps [42], and real estate/intelligence. other wisdom. We take the field of art as an example. First, artists traditionally have very few channels to display their work. The price may not reflect the true value of their work due to a lack of interest. Worse still, their work published on social networks was charged intermediaries by platforms and advertisers. NFTs convert their work to digital formats with embedded identities. Artists do not have to transfer ownership and content to agents. This gives them a boost with lots of profit. Good examples include Mad Dog Jones' REPLICATOR (sold for $4.1 million [29]), works by Grimes (sold for a total of about $6 million [23]), and other works by pre-money artists top electronics like Beeple [45]/Trevor Jones [50]. In addition, artists are often unable to collect royalties from future sales of their work. Conversely, NFTs can be programmed in such a way that artists receive a pre-determined royalty each time their digital work is traded in the marketplace (e.g., SuperRare [47], MakersPlace [30], Rare Art Lab [42], VIV3 [51]). It is an effective way to manage and protect digital masterpieces. Furthermore, some platforms (e.g., Mintbase [34], Mintable [33]) even implement tools to make it easy for ordinary people to create their own NFT works.

Inspiring the Metaverse. Metaverse is a collective shared virtual space that enables all kinds of digital activity. In general, it includes a variety of techniques such as augmented reality and the internet to establish virtual worlds. The concept originated decades ago and has come a long way with the rapid development of blockchain. Blockchain provides an ideal decentralized environment for the online virtual world. Participants in these blockchain- powered alternative realities can have a variety of compelling use cases, such as enjoying games, displaying homemade artwork, exchanging assets and virtual assets (art, land, names, video photos, mobile objects), and so on. In addition, users also have the opportunity to benefit from the virtual economy. They can lease buildings (such as offices) to others for bail or breed rare pets and sell them for rewards. The main blockchain-based projects are Decentraland [65], Cryptovoxels [18], Somnium Space [45], MegaCryptoPolis [32], and Sandbox [3]. The metaverse ecosystem includes all the

applications. We list it separately here simply because it is still in the early stages due to its complexity.

CHALLENGES

To enable the development of NFT applications, a series of obstacles must be overcome, as with any developing technology. We discuss some typical challenges from a usability, security, governance, and scalability perspective, including system-level issues caused by blockchain-based platforms and blockchains. Human factors such as government, regulation, and society.

Usability Challenges

Usability is a measurement of the effectiveness, efficiency, and satisfaction of a user when testing a particular product/design. Most NFT systems are built on Ethereum. Therefore, there are still major downsides to Ethereum. We tackle two major challenges that have a direct impact on user experience.

6.1.1 Slow Confirmation. NFT-related procedures are usually conducted by sending transactions through smart contracts for reliable and transparent management (such as minting, selling, and exchanging). However, current NFT systems are tightly coupled to their underlying blockchain platforms, making them low in performance [Bitcoin only hit 7 Ticks Per Second (TPS) [89] while Ethereum only hit 30 TPS]. This results in extremely slow NFT confirmations. Conquering this challenge requires an overhaul of the blockchain system [93], optimization of its structure [71][90], or improvement of consensus mechanisms [57]. Existing blockchain systems cannot accommodate such requirements.

High Gas Price. High gas prices have become a major problem for the NFT market, especially since large-scale NFT mining requires metadata to be uploaded to the blockchain network. All NFT-related transactions are more expensive than a simple transfer because smart contracts involve computational and storage resources to process. At the time of writing, mining NFT tokens costs more than $100 (or about 33×109wei)1. To make a simple NFT transaction it can cost anywhere from $100 to $500 per transaction. High fees caused by complex operations and high congestion severely limit wide-scale adoption.

Security and Privacy Issues

The security of user data is the top priority of the systems. However, data (stored off-chain but linked to an on-chain token) runs the risk of being lost or misused by malicious parties. We provide the following details.

NFT Data Inaccessibility. In traditional NFT projects, a cryptographic "hash" as an identifier, instead of a copy of the file, is tagged with a token and then saved on the blockchain to save on gas consumption. This causes users to lose confidence in NFT because the original file can be lost or corrupted. Some NFT projects integrate their systems with a specialized file storage system such as an Inter Planetary File System (IPFS) [58], where an IPFS address allows a user to find a piece of content if someone somewhere on the IPFS network stores it. Certainly, such systems are flawed. When users "upload" NFT metadata to IPFS nodes, there is no guarantee that their data will be replicated to all nodes. Data may not be available if the content is stored on IPFS and the only node storing it is disconnected from the network [59]. This issue has been reported by DECRYPT.IO [59] and CHECKMYNFT.COM [62].

Also, an NFT could point to the wrong file address. If so, the user cannot prove that they own the NFT. In short, relying on an external system as a core (storage) component of 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 underlying 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 to the public. Otherwise, all the activities of users under the exposed address are observable. Existing privacy-preserving solutions (e.g., homomorphic encryption [92], zero-knowledge proof [94], ring signature [81],

multiparty computation [82]) have not been yet applied to the NFT related schemes due to their complicated cryptographic primitives and security assumptions. Like other types of blockchain-based systems, reducing expensive computation costs becomes key to implementing privacy-preserving systems.

-

Governance Consideration

Like the situation with most cryptocurrencies, the NFT also faces obstacles such as strict government regulation. On the other hand, how to adapt this nascent technology to the respective market is also a challenge. We discuss two issues typical of both sides.

Legal Pitfalls. NFTs face legal and policy issues in many areas [53][74]. Potentially affected areas include cargo, cross-border transactions, KYC (Know Your Customer) data, and more. It is important to understand regulatory review and related legal action before moving to NFT tracks. In some countries, such as India and China, the regulatory situation is as strict for cryptocurrencies, as for the sale of NFTs. The exchange, transaction, purchase, and sale of NFT must overcome administrative difficulties. Legally, users can only trade derivative products on authorized exchanges such as stocks and commodities, or trade tokens with someone personally. Some countries, such as Malta and France, are trying to come up with appropriate laws to regulate the service of digital assets. Elsewhere, issues are resolved using applicable laws. They oblige the buyer to respect complex and even contradictory terms. Therefore, doing due diligence is a must before investing serious tokens in NFT.

Taxable Property Issues. Intellectual property products (including works of art, books, domain names, etc.) are considered taxable property under the applicable legal framework. However, NFT-based sales are still outside this range. Although some countries, such as the United States (Internal Revenue Service, IRS), tax cryptocurrencies as property, most parts of the world do not consider it yet. This can significantly increase financial crime under the guise of NFT transactions.

1 Source calculated from https://www.coinmarketcap.com/ and https://www.ethereum.org/en/developers/docs/gas

Governments want to make selling NFTs more credible with tax consequences. Specifically, individual participants are subject to capital gains tax on NFT assets. In addition, exchanges NFT for NFT, NFT for IP, and Eth for NFT (or vice versa) must be taxed. Also, for high-yield properties or collectibles, a higher tax bracket should apply. Therefore, professions related to NFT should seek further advice from professional tax services after in-depth discussion.

Extensibility Issues.

The scalability of NFT schemas is twofold. The first is to highlight whether a system can interact with other ecosystems. The second focuses on the ability of the NFT system to receive an update when the current version is dropped.

NFT Interoperability(cross-chain). The current NFT ecosystems are isolated from each other. Once users select a product type, they can only sell/buy/trade them within the same

ecosystem/network. This is due to its underlying blockchain platform. Interoperability and cross-chain communication remain
limitations for large-scale adoption of DApps. Based on our observations [100], cross-chain communication can only be done with the help of trusted external parties. Decentralized ownership, in this way, has certainly been lost to some extent. But fortunately, most of the projects related to NFT use Ethereum as their underlying platform. This shows that they share a similar data structure and are tradable according to the same rules.

Updatable NFTs. Forward blockchains update their protocols through soft forks (small changes compatible with newer versions) and hard forks (significant changes that may conflict with previous protocols). A formal discussion has been provided showing [63] the difficulties and trade-offs of applying updates to an existing blockchain. Despite using a generic model, new releases still face tough requirements such as tolerating specific conflicting behaviors and staying online during updates. NFT systems depend heavily on their underlying foundations and remain consistent with them. While data is usually stored in separate components (such as the IPFS file system), the most important logic and TokenId are still stored on-chain. Updating the system appropriately with improvements will be a necessity.

CONCLUSION

Non-Fungible Token (NFT) is an emerging technology that is prevalent in the blockchain market. In this report, we explore cutting-edge NFT solutions that could reshape the virtual/digital asset market in the future. We first analyze the technical components and provide design patterns and properties. Next, we evaluate the security of current NFT systems and discuss in more detail the opportunities and potential applications of the NFT concept. Finally, we describe existing research challenges that need to be addressed before mass-market penetration is achieved. We hope this report provides timely analysis and summaries of existing proposed solutions and projects, making it easier for new entrants to track current progress.

REFERENCES

Alien Worlds. Project Accessible. 2021. [https://www.alienworlds.io/]

Art Blocks. Project Accessible. 2021. [https://artblocks.io/]

Async Art. Project Accessible. 2021. [https://async.art/]

Axie Infinity. Project Accessible. 2021. [https://axieinfinity.com/]

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).

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., et al. "A next-generation smart contract and decentralized application platform." White paper 3(37) (2014).

Beeple. Project Accessible. 2021. [https://www.beeple-crap.com/]

Bored Ape Yacht Club. Project Accessible. 2021. [https://boredapeyachtclub.com/#/]

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).
Ciampi, M., et al. "Updatable blockchains." In: European Symposium on Research in Computer Security. pp. 590–609. Springer (2020).
Cargo. Project Accessible. 2021. [https://cargo.build/]
Coingecko website. Accessible. 2021. [https://coingecko.com/en]
Cometh. Project Accessible. 2021. [https://www.cometh.io/]
Crypto stamp. Project Accessible. 2021. [https://crypto.post.at/]
Cryptocats. Project Accessible. 2021. [https://cryptocats.thetwentysix.io/]
Cryptokitties. Project Accessible. 2021. [https://www.cryptokitties.co/]
Cryptopunks. Project Accessible. 2021. [https://www.larvalabs.com/cryptopunks]
Cryptoslam. Project Accessible. 2021. [https://cryptoslam.io/]
Cryptovoxels. Project Accessible. 2021. [https://www.cryptovoxels.com/]
Cryptowine. Project Accessible. 2021. [https://grap.finance/#/]
Dappradar website. Accessible. 2021. [https://dappradar.com/]
Decentraland (MANA). Project Accessible. 2020. [https://decentraland.org/].
Fabian, V., Vitalik, B. "Eip-20: Erc-20 token standard." Accessible: [https://eips.ethereum.org/EIPS/eip-20] (2015).
Fast box. Project Accessible. 2021. [https://www.fastbox.org/]
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. "The bitcoin backbone protocol: Analysis and 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 Communications Security. pp. 3–16. ACM (2016).
Grimes sold $6 million worth of digital art as NFTs. News source. 2021. [https://www.theverge.com/2021/3/1/22308075/grimes-nft- 6-millionsales-nifty-gateway-warnymph]
Gods Unchanged. Project Accessible. 2021. [https://godsunchained.com/]
Gudgeon, L., Moreno-Sanchez, P., Roos, S., McCorry, P.,
Gervais, A. "Sok: Layertwo blockchain protocols." In:
International Conference on Financial Cryptography and Data
Security. pp. 201–226. Springer (2020).
Hashmasks. Project Accessible.
2021. [https://www.thehashmasks.com/]
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).
Icecap. Project Accessible. 2021. [https://icecap.diamonds/] 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).
Known Origin. Project Accessible. 2021.

[https://www.knownorigin.io/]
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). Loot contract code. [https://etherscan.io/address/0xff9c1b15b16263c61d017ee9f65c 50e4ae0113d7#code] 2021.
Loot talk. [https://loot-talk.com/] 2021.
Mad Dog Jones. News source. 2021. [https://www.phillips.com/detail/mad-dog-jones/NY090121/1]
Makersplace. Project Accessible. 2021. [https://makersplace.com/]
Meebits. Project Accessible. 2021. [https://meebits.larvalabs.com/]
Megacryptopolis. Project Accessible. 2021. [https://mcp3d.com/]
Menezes, A.J., Van Oorschot, P.C., Vanstone, S.A. Handbook of Applied Cryptography. CRC press (2018).
Mintable. Project Accessible. 2021. [https://mintable.app/]
Mintbase. Project Accessible. 2021. [https://www.mintbase.io/]
Moore, D., Voelker, G., Savage, S. "Inferring internet denial-of-service activity." ACM Trans. Comput. Syst. 24, 115–139 (2006).
Mycryptoheroes. Project Accessible. 2021. [https://www.mycryptoheroes.net/]
Nakamoto, S. "Bitcoin: A peer-to-peer electronic cash system." Tech. rep., Manubot (2019).
NBA Top Shot. Accessible. 2021. [https://nbatopshot.com/]
Nft bank. Project Accessible. 2021. [https://nftbank.ai/]
Nifty gateway. Project Accessible. 2021. [https://niftygateway.com/]

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

Nonfungible website. Accessible. 2021. [https://NonFungible.com]
Opensea platform. Accessible. 2021. [https://opensea.io/]

Raman, R.K., et al. "Trusted multi-party computation and verifiable simulations: A scalable blockchain approach."arXiv preprint arXiv:1809.08438 (2018).
Rarible. Project Accessible. 2021. [https://rarible.com/]

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, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance." In: FSE. pp. 371–388. Springer (2004).
R planet. Project Accessible. 2021. [https://rplanet.io/]

R.a.r.e art lab. Project Accessible. 2021. [https://www.lagelnd.com/rare]
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@ MoDELS2008 (2008)

Szabo, N. "Smart contracts: Building blocks for digital markets." EXTROPY: The Journal of Transhumanist Thought, (16) 18(2) (1996).
Skyweaver. Project Accessible. 2021. [https://www.skyweaver.net/]
Somnium space. Project Accessible. 2021. [https://somniumspace.com/]
Sorare. Project Accessible. 2021. [https://sorare.com/]
Superrare. Project Accessible. 2021. [https://superrare.co/]
Topps MLB. Project Accessible. 2021. [https://toppsmlb.com/]
Tradestars. Project Accessible. 2021. [https://tradestars.app/]
Trevorjonesart. Project Accessible. 2021. [https://www.trevorjonesart.com/]

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).

Viv3. Project Accessible. 2021. [https://VIV3.com]

Wax: Worldwide Asset Exchange. Accessible. 2021. https://on.wax.io/wax-io/]
EOS. Accessible. 2018. [https://eos.io/]
Wang, G., et al. "Sok: Sharding on blockchain." InProceedings 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 standard." Ethereum Improvement Protocol, EIP- 721, Accessible:
[https://eips.ethereum.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, Accessible: [https://eips.ethereum.org/EIPS/eip-1155] (2018).

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

Zora. Project Accessible. 2021. [https://zora.co/]
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).

Appendix A. NFT Security