JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue

JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)

An International Scholarly Open Access, Peer-reviewed, Refereed Journal

NON-FUNGIBLE TOKEN (NFT): OVERVIEW, OPPORTUNITIES AND CHALLENGES

[1]Teslin Seby V
[1]Assistant Professor
[1]Commerce,
[1]Don Bosco College, Mannuthy, Kerala, India

Abstract : The Non-Fungible Token (NFT) market is mushrooming 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. The thousand fold 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. This study mainly aims to explain technical terms, security threats, opportunities and challenges of this investment alternative

Index Terms - **NFT, Ethereum, Decentralized application.**

I. INTRODUCTION

Non-Fungible Token (NFT) is a type of crypto currency 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 crypto currencies such as Bitcoin in their intrinsic features. Bitcoin is a standard coin in which all the coins are 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, 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 become a promising intellectual property (IP)-protection solution. Although, in essence, NFTs represent little more than code, but the codes to a buyer have a scribed 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. 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.

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 tackled, 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 study aims at detailed analysis of technical components, security threats and some opportunities and threats for NFT investment.

II. OBJECTIVES OF THE STUDY

- To familiar with technical terms involved in NFT investment
- A security evaluation of current NFT systems.
- To analyse opportunities and challenges of NFT investment.

III. 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 because 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, Hyper ledger, 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 crypto currencies. 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 with a correct digital signature. This simple operation is usually performed using a crypto currency 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 quality/resolution. In the mainstream blockchain systems such as Bitcoin and Ethereum, 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 he owns the NFT-based intellectual property, 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.

IV. 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, which covers all security aspects of a system: authenticity, integrity, non-reputability, availability and access control. We investigate the potential security issues and propose some of the corresponding defense measures to address these issues.

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 unforgetability 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 exposed to unauthorized users, which violates confidentiality. 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.

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 violate 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, 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.

V. 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 Crytpo Kitties, Cryptocats, Crypto Punks, Meebits, Axie Infinity, Gods Unchanged, and Trade Stars. 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 function 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, digital images, videos, virtual real estate, domain names, 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.

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

VI. 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.

Slow Confirmation

NFT-related procedures are typically conducted by sending transactions via the smart contract for reliable and transparent management. However, current NFT systems are closely coupled with their underlying blockchain platforms, which makes them suffer from low performance. This result 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 fulfill such requirements.

NFT Data Inaccessibility

In the mainstream NFT projects, 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 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.

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 by the public. Otherwise, all the activities of users under the exposed address are observable. Existing privacy-preserving solutions 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.

Legal Pitfalls

NFTs confront legal and policy issues across a wide range of areas. Potential concerned areas cover commodities, cross-border transactions, KYC 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 crypto currencies, 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 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 crypto currencies 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.

NFT Interoperability

Existing NFT ecosystems are isolated 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.

VII. 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. Firstly analyze the technical

components and provide the design models and properties. Then, tried evaluate the security of current NFTs systems and further discuss the opportunities and potential applications that adopt the NFT concept. A new investment opportunity NFT system is less familiar among public so the report tried to study the terms, opportunities and challenges of this investment option may enlighten further analysis.

REFERENCES

[1]. Ante, L., 2021. Smart Contracts on the Blockchain – A Bibliometric Analysis and Review. Telemat. Informatics 57, 101519.

[2]. Dowling, M., 2021b. Fertile LAND: Pricing non-fungible tokens. Finance. Res. Lett. 102096.

[3]. Nadini, M., Alessandretti, L., Di Giacinto, F., Martino, M., Aiello, L.M., Baronchelli, A., 2021. Mapping the NFT revolution: market trends, trade networks and visual features.

[4]. Non Fungible, 2021. NFT Market History [WWW Document]. URL https://nonfungible.com/market/history (accessed 3.29.21).

[5]. Reuters, 2021. EBay says open to accepting to cryptocurrencies in future, exploring NFTs [WWW Document]. URL https://www.reuters.com/technology/ebay-ceo-says-looking-cryptocurrency-payment-option-cnbc-2021-05-03 (accessed 5.3.21).