

# Towards a secure and trustworthy imaging with non-fungible tokens

Nicolas Martinod<sup>a</sup>, Kambiz Homayounfar<sup>b</sup>, Davi Lazzarotto<sup>a</sup>, Evgeniy Upenik<sup>a</sup>, and  
Touradj Ebrahimi<sup>a</sup>

<sup>a</sup>Multimedia Signal Processing Group (MMSPG), École Polytechnique Fédérale de Lausanne  
(EPFL), Lausanne, Switzerland

<sup>b</sup>RayShaper SA, Crans-Montana, Switzerland

## ABSTRACT

Non-fungible tokens (NFTs) are used to define the ownership of digital assets. More recently, there has been a surge of platforms to auction digital art as well as other digital assets in form of image, video, and audio contents of all sorts of purposes ranging from collectibles to means of investment. Although NFTs have the potential of revolutionizing the foundations of ownership and possession of digital assets, they also face various challenges in terms of trust, security as well as legal implications and even social acceptance. This paper identifies the main challenges in NFTs and discusses potential directions in order to remedy to their current shortcomings, with emphasis on digital assets in form of images.

## 1. INTRODUCTION

Non-fungible tokens (NFTs) have become a popular mechanism to enable innovative ecosystems of values not only in the digital world but also affecting several more traditional approaches in the physical world. At the time of this writing, the jury is still out in fully understanding the extent of the impact of NFTs. While some compare the invention of NFT to other major revolutions in information and communication technologies such as the Internet, the World Wide Web or the Social Networks, others dismiss it as a passing fashion that will soon fade away, to become a shadow of itself similar to rotary phones and slide rules. The goal of this paper is to provide an overview of key elements of NFTs to imaging and media experts. The rationale behind this objective is that currently most technical players in NFT are experts in computer science, security and distributed systems, while most digital assets in form of NFTs are multimedia contents and in particular in form of image, video and sometimes audio. Exposure of NFTs to imaging and media experts can open doors to more efficient and better tools taking into account also characteristics of the digital assets in form of media and images. The paper is organized as follows. The concept of tokenization of digital assets is presented next and in particular the non-fungible tokens by providing a number of use cases that have been identified as potential beneficiaries of NFTs. After presenting the workflow of minting NFTs and their transactions as they are implemented today, we will discuss some of the key challenges regarding NFTs. We then concentrate on the solution to one of those challenges, namely, interoperability and longevity, by discussing standardization of NFTs and what JPEG standardization committee is undertaking in order to define a standard that takes advantage of characteristics of digital assets in a more efficient manner than it is done today.

## 2. TOKENIZATION OF DIGITAL ASSETS

Tokens are a widely employed method to define possession of an item or right to a service. Certificates of title, for instance, are used to prove that assets such as real-estate properties belong to its rightful owner since long before the advent of the Internet. Other documents, such as diplomas, can serve as tokens attesting that their owners successfully completed the conditions to acquire them and possess an expected set of skills. These concepts have lately been extended to the digital world, and digital tokens are increasingly employed in many applications. Badges<sup>1</sup> are an important example of such digital tokens, and are employed to validate that an individual, an entity or an object possesses a particular set of skills, knowledge, qualifications or quality according to a pre-defined criteria. Cryptocurrencies, such as bitcoin,<sup>2</sup> are an important category of fungible tokens, being classified as such, because each individual unit of the asset is identical in value to any another and can be exchanged against

it. On the other hand, non-fungible tokens have the feature of being provably scarce, which requires them to depend on a mechanism that can reliably assert of their uniqueness along with its ownership or possession rights. It is important to note that such non-fungible tokens can also be defined for physical assets either directly or for their digital twin. For instance a physical Swiss Frank bill is equivalent to a cryptocurrency in the digital world, both representing fungible assets. A certified piece of art, such as a painting in the physical world, is comparable to an NFT pointing to a unique digital picture which is either a scanned version of the latter or created by an artist from scratch in the digital world. An electronic proof of vaccination such as a Covid pass is similar to a physical attestation confirming that the named individual has been vaccinated. Figure 1 depicts the different types of tokens both in digital and in physical world and their relationships.







	Fungible	Non-fungible	Badge
Physical			
Digital			

Figure 1. Diagram depicting the concept of tokens in form of examples for digital assets and physical objects. The top center image is a picture of the painting "Le Lac de Thoune aux reflets symétriques" by the Swiss painter Ferdinand Hodler and is a courtesy from JI FilpoC [CC BY-SA 4.0 (<https://creativecommons.org/licenses/by-sa/4.0/deed.en>)]. The bottom central image is a recreation of the "Nyan Cat" and is a courtesy from Rob Bulmahn [CC BY 2.0 (<https://creativecommons.org/licenses/by/2.0/>)]. The top right image is the picture of a Swiss passport and is a courtesy from Item [CC BY-SA 3.0 (<https://creativecommons.org/licenses/by-sa/3.0/legalcode>)].

## 2.1 Non-Fungible Tokens

When the first NFT standard was proposed, cryptocurrencies were already quite popular around the globe. As one of the most popular implementations of blockchain, Ethereum<sup>3</sup> had previously proposed the ERC-20<sup>4</sup> standard, which allowed for the implementation of digital tokens through smart contracts. Tokens created using this standard were fungible, meaning that as defined above, each instance is the same as any other in regards to both type and value. Since such a representation was not adequate to typify unique assets, the Ethereum Improvement Proposals (EIP)-721<sup>5</sup> was issued to define NFT. Contrary to previous tokens, each instance of an NFT is uniquely distinguishable, which is a pre-requisite for proof of possession or ownership.

Several technical elements are essential for practical implementations of NFTs, such as the blockchain and smart contract. The blockchain is the primary mechanism allowing to securely keep information about the transfer record of an NFT without the need for a centralized trusted entity. Ethereum<sup>3</sup> is the most used platform to append information to the blockchain and currently relies on the Proof of Work (PoW)<sup>6</sup> as consensus mechanism which is known to demand large amount of electricity to operate. This has resulted in the use of less power hungry alternative platforms such as Tezos<sup>7</sup> which are gaining in popularity due to the lower energy consumption of their consensus mechanism based on Proof of Stake (PoS).<sup>8</sup> The same blockchain architectures also serve as basis for the implementation of smart contract,<sup>9</sup> which is the framework employed in all NFT operations. Smart contract define a number of functions that can be used to transfer an NFT, verify its owner

or possessor, as well as several other functionalities such as conditions of transfer and any potential restrictions associated with the latter.

The unique features of NFTs have already been exploited in many use cases, while other applications have been hypothesized but not yet fully explored. A non-exhaustive list of such use cases can be found here:

- **Digital artwork:** This is probably the most prominent use case for NFTs at present. Everyday, artists and creators mint their work of art to the blockchain as NFTs and transfer them to interested buyer through a bid or for a stipulated price. The blockchain keeps track of the transfer record over time, allowing to grant royalties to the original creator at each subsequent transfer. On March 2021, the sale of "Everydays: the first 5000 days" for 69.3 Million dollars set the record for the most expensive NFT sale.<sup>10</sup>
- **Collectibles:** As one of the early examples of NFTs in Ethereum, the Cryptopunks<sup>11</sup> are a collection of ten thousand unique virtual characters. If initially users could claim a cryptopunk for free at the moment they were created, the market for these 28 x 28 pixel avatars has now moved to a total surpassing 400 Million dollars<sup>12</sup> in sales. The huge monetary value of this and other NFT-based collections such as NBA Top Shot,<sup>13</sup> Bored Ape Yacht Club<sup>14</sup> or the Meebits<sup>15</sup> demonstrate that proposed solutions based on NFTs are well adapted to this use case.
- **Games:** The gaming industry has already been taking advantage of interesting properties of NFTs inside their virtual worlds, employing them to represent items that can be collected and traded with other players. This mechanism allows for an environment less dependent of game developers, where the virtual universe stays operable as long as there are active players. Such systems have attracted thousands of curious gamers and interested investors to platforms such as Axie infinity,<sup>16</sup> CryptoKitties<sup>17</sup> and Decentraland,<sup>18</sup> creating living virtual economies that have generated more than 650 Million dollars so far.<sup>12</sup>
- **Micro licensing:** The rise of NFTs as a mean to sell digital artistic work has initiated a discussion about what exactly a person receives upon the acquisition of an NFT. The NFT license,<sup>19</sup> adopted by the CryptoKitties<sup>17</sup> was one solution proposed to resolve this issue, which reserved the copyrights to the creator while allowing the NFT possessor to use his/her property for both non-commercial and commercial use, given that the generated revenue is no more than 100 thousand dollars per year. However, new mechanisms have been proposed on the music market where the creator would sell copyright shares of his/her work, allowing the NFT buyers to receive royalties on his creation. This mechanism has been proposed in platforms such as Bluebox,<sup>20</sup> but hasn't been explored to its full potential so far.

## 2.2 Current implementation of NFTs

An NFT is a smart contract linking a token to a digital asset. This smart contract lives on a blockchain ("on-chain") and users can interact with it according to the set of rules defined within that contract. The current workflow for NFT implementation is shown in the diagram below.

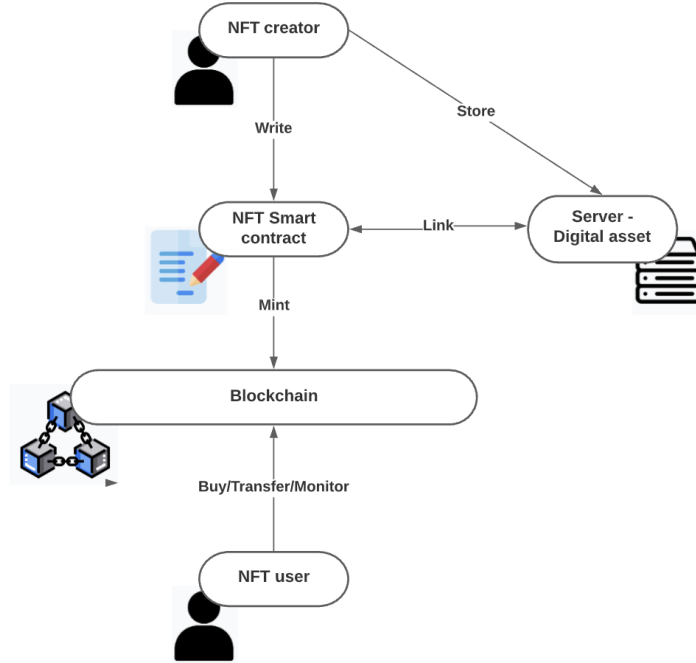


Figure 2. NFT workflow from creation to storage to transaction.

The NFT creator creates a smart contract. The smart contract needs to follow a standard, i.e: ERC-721,<sup>5</sup> in order to allow for interoperability with all NFT-based platforms and tools compliant with that standard. However, in current standards the creator is allowed to encode additional requirements in form of metadata in the smart contract. As storing data on a blockchain is costly, the digital asset need is often stored off-chain because of its large volume. Thus, a robust link between the off-chain digital asset and the on-chain NFT is crucial and should be defined and implemented within the smart contract.

For the storage of a digital asset off-chain, a centralized or decentralized storage architecture can be used. One issue with centralized storage is that it uses an URL, which are location-based addressing - meaning it is just a path pointing toward the exact location of the asset . However, while the URL cannot be changed, a malicious actor can potentially tamper with the digital asset to which the URL is pointing. A solution to this problem is to use a CID (content identifier) instead of a URL, which uses content-based addressing. An example of a CID can be the hash value of the digital asset. A popular solution to decentralized storage is the IPFS<sup>21</sup> , Filecoin<sup>22</sup> or Arweave.<sup>23</sup>

Once written, the smart contract can be deployed on a blockchain and the NFT can be minted. Once minted, the NFT owner can transfer or sell it to anyone by recording the transaction on the blockchain in a similar way transactions of cryptocurrencies are added to a blockchain.

### 2.3 Example of minting an NFT

A concrete and typical example of NFT implementation is shown in the diagram below. This implementation, which was carried out in the framework of ProCam, an EPFL multidisciplinary educational project sponsored by MAKE, is similar to many current approaches for creation of NFTs and enjoy the same advantages and drawbacks of the state of the art in this domain.

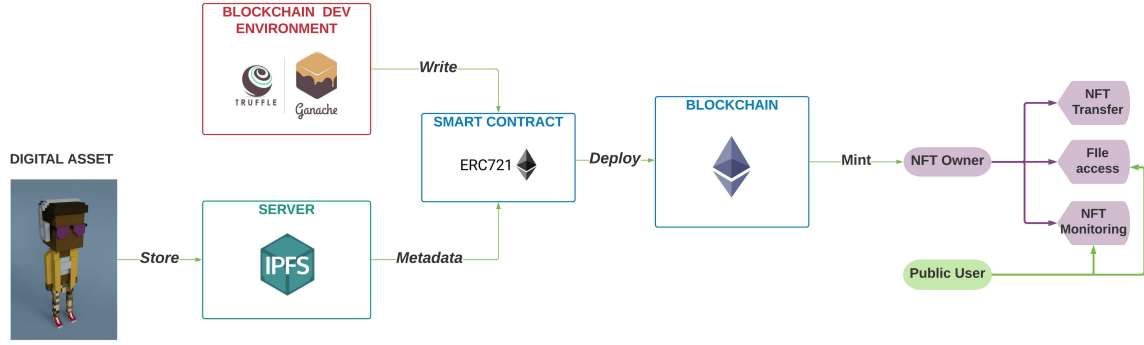


Figure 3. A concrete and typical example of minting an NFT

As in any other NFT implementation, it requires a blockchain development environment, such as Truffle<sup>24</sup> or Hardhat,<sup>25</sup> and a personal blockchain to run tests, such as Ganache<sup>26</sup> (though Hardhat has a built-in network for this).

The smart contract was written according to the leading standard, ERC-721.<sup>5</sup> As in many other use cases, it relies on OpenZeppelin<sup>27</sup> contracts to obtain a low-risk and up-to-date NFT.

Our digital asset, in form of a picture, is stored on a decentralized, URI-based server, IPFS.<sup>21</sup> The stored file metadata can then be used to link the digital asset to the smart contract created as described above. The ERC-721 standard includes a method called tokenURI to tell applications where to find the metadata for a given item. The tokenURI method returns a public URL, which returns a JSON file containing metadata for a digital asset.

Once created, the smart contract can be deployed to the Ethereum blockchain and the NFT is then minted. The owner of the NFT is the sole user allowed to transfer the NFT to another user. As the ethereum blockchain and IPFS network are both publicly accessible, any user can also view the digital file and monitor all NFT transactions.

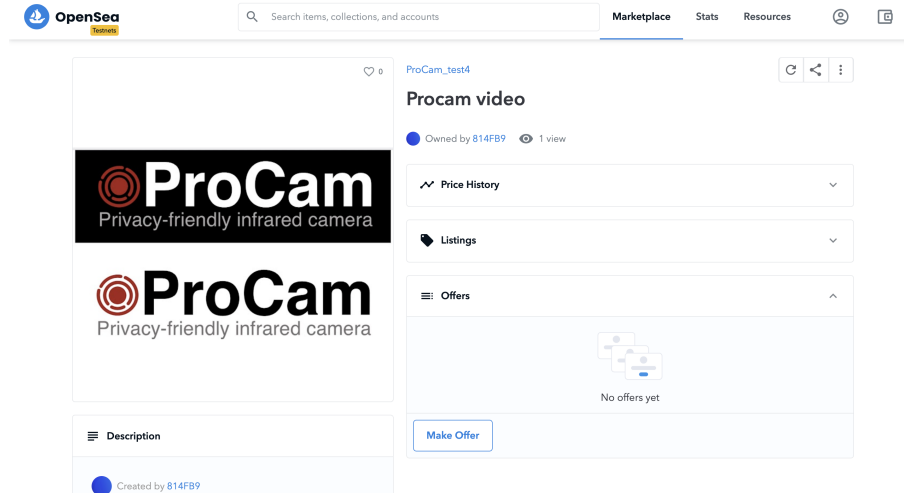


Figure 4. Example of an NFT in form of a digital picture, displayed on Opensea marketplace.

### 3. CHALLENGES IN NFTS

Despite a growing number of implementations in form of platforms for minting NFTs and their exchange, a large number of issues still remain open which hinder their wider and faster adoption. In this section we address some

of the major ones and discuss them.

### 3.1 Trustworthiness

As defined before, NFT, in effect, is a certificate combined with a smart contract and some metadata such as a name, a textual description, or an image. The authenticity of the certificate in NFTs is not, as usually the case in both physical and digital worlds, through a trusted third part, but through a zero trust mechanism relying on a decentralized networks of nodes that work based on a consensus mechanism similar to how most cryptocurrencies operate, namely, the blockchain. The first and central question behind any certificate is how much one can trust it. Although, such a trust is directly related to the level of security put in place to protect the certificate against forgery and fraud, it is not quite the same as trust which includes other real or perceived dimensions. For instance, in the case of more traditional certificates based on a trusted third party such as a governmental agency or a bank, the trust on the certificate largely depends on the degree of trust on the entity issuing that certificate. In certificates that rely on decentralized network such as a blockchain, there is no third party of trust involved which is replaced by the decentralized network as a whole and how a consensus is reached through a complex and often perceived as obscure mechanisms, not well understood by general public. The trust then becomes dependent on how much an individual or an organization trusts the network itself. Note that this is not a purely technical issue and often includes much more complex social and psychological considerations that play a role in defining trust. A good illustration of trust, or rather its lack, is the initial resistance of consumers to the use of electronic payment systems in the early days of the world wide web, a key element behind the growth in e-commerce. Such a resistance (which was mainly driven by a lack of trust) was overcome by a combination of efforts, protocols, law and above all, when users gradually learned how to use and then trust online payment systems. The same journey still needs to be completed in the case of NFTs before a sufficient degree of trust is installed in the consumers.

### 3.2 Security and privacy issues

Security features of an NFT system should in principle cover six issues: authenticity, integrity, non-repudiation, confidentiality, availability and access control.

Authenticity is vulnerable to spoofing, which is the ability to impersonate another person or computer on the system. When a user interacts with the blockchain to mint or sell NFTs, a malicious attacker may steal the user's private key to illegally obtain the ownership of his/her NFTs. How does the user prevent the leakage of the private key? Can cold storage help?

Integrity is vulnerable to tampering, which refers to the malicious modification of either the NFT data or the digital asset it refers to. The metadata and ownership of NFTs cannot be maliciously modified after the transaction is confirmed on the blockchain. Yet, the NFT data stored outside blockchain may be maliciously manipulated. Can this vulnerability be resolved by the seller sending both the hash data in addition to the original data to the NFT buyer?

Non-repudiation associates a person to a fact, making it impossible for them to deny that something happened. The fact that a user sends an NFT to another user, in particular, cannot be denied. This is guaranteed by the security of the blockchain and its unforgeable nature. However, it has been demonstrated that under certain circumstances, security of a blockchain can be compromised. IN particular, further research is necessary to determine if implementing a multi-signature contract, which requires confirmation of each binding by several participants, could resolve the non-repudiation issues associated with NFTs in a number of use cases.

Confidentiality is the vulnerability to information leakage, which occurs when unauthorized individuals obtain access to sensitive data. In NFT systems, the state information and code in smart contracts are entirely transparent, and any state and its changes are publicly visible to any observer. Even if the user adds the NFT hash to the blockchain, a malicious attacker can readily exploit the link between the hash and transaction. Could NFT sellers circumvent this issue by deploying privacy-preserving smart contracts rather than standard smart contracts?

Availability can be compromised by Denial of Service (DoS) attacks whereby a malicious attacker makes a server unavailable or interrupts the normal functions. Even though blockchain ensures high degrees of service

availability, a hostile actor can employ DoS to attack centralized web applications or raw data outside the blockchain, causing NFT traders to experience a denial of service.

Access control, also known as authorization, is vulnerable to malicious manipulation of a user's legitimate privileges. In NFT systems, an attacker could jeopardize a genuine user's selling permissions, which are provided via a basic smart contract.

### **3.3 Interoperability and longevity issues**

Many NFT implementation already rely on a number of standards that are briefly presented in the next section. Unfortunately, most such standards require their implementation to be on a specific blockchain and do not take advantage of the nature and format of the digital asset they refer to. In addition to lack of leverage on the specific standard format in which a digital asset is represented, most NFT platforms create their own proprietary metadata both in types and in representations, and store them either off-chain or on-chain, breaking full interoperability between different implementations of NFTs. Beside fragmentation of NFT market, this results in a serious concern regarding longevity of the NFTs in future because if the organization behind a specific NFT platform disappears, then there will not be a guarantee that the NFTs minted using that platform will be fully decodable and crucial information about such NFTs might disappear. A complete standard that not only allows for cross-chain interoperability but also enables specifications of the additional metadata and at the same time takes advantage of the digital asset formats is a must and remains a challenge currently.

### **3.4 Legal issues**

The art world is a complicated web of stakeholders who collaborate and compete to create, show, conserve, promote, and trade works of art. As modern enablers of the art business, NFTs inherit a slew of legal issues, the most significant of which remain unresolved.

The first legal issue is ownership and the form of ownership implied by possession of an NFT. The answer is contingent upon the nature of the underlying asset represented by the NFT. An NFT may be the original asset or one that exists exclusively in the digital and therefore virtual world. At the same time, an NFT can serve as an ownership certificate of a physical asset, such as a painting.

Second, from the perspective of a content creator, NFT is a lifesaver. An NFT recorded on the blockchain ensures the immutability and uniqueness of digital content, enabling artists to safeguard their works against forgery and duplication. Thus, blockchain-registered NFTs can potentially address the issues of digital piracy and high intermediation costs. Nonetheless, not all creators possess absolute, exclusive rights to their work. The rights to an artwork are often divided among numerous parties, with one party controlling distribution, another controlling exhibition, another controlling performance, and yet another controlling marketing. This shared-rights ecosystem raises the question of who has the authority to establish the NFT.

Thirdly, the rights of the NFT purchaser are at stake, and the old adage "buyer beware" applies. Purchasing an NFT does not automatically confer ownership of the artwork's intellectual property. For example, buying a book gives the buyer the right to read it, show it to friends, and keep it on the buyer's bookshelf; it does not grant the customer the right to photocopy or freely quote from the book. The same is true when purchasing an NFT pointing to a digital asset, unless the purchase agreement expressly states that the buyer has additional specified rights.

Many of the legal issues highlighted above in the context of the art as a use case, remain valid in other use cases which often also include their own further legal issues. The legal aspects of NFTs is currently an uncharted territory and at present most legal considerations aim at protecting the operators of the platform for NFTs, and seldom considers rights and protections of the creator or the buyer of NFTs. In fact, even the so-called legal protections of the operators of the platforms are not guaranteed to be considered valid in a court of law.

### 3.5 Environmental issues

In several use cases, and in particular in the art market, the advantages of NFTs which can cut the intermediaries and open doors for artist to new channels of access buyers, are offset by ecological considerations that slow down or even prevent their wider adoptions. This is mainly motivated by the fact that many blockchain on which NFTs operate are large consumers of energy which in turn have a negative impact on the environment especially if the source of the energy used for their operations is fossil based. Such considerations should be taken seriously but also with the necessary precautions. It is important to keep in mind that tremendous progress has been made recently in the design and implementation of blockchain architectures that are much less energy hungry than the previous generation and this trend is continuing. Nevertheless, the quest for more environmental friendly solutions to implement without compromising their security or efficiency is a challenge that remains to be resolved.

## 4. NFT STANDARDS

NFT standards describe the specific attributes of smart contracts for non-fungible tokens. This section describes NFT standards introduced by Ethereum, the most popular blockchain in NFTs, and Tezos, an alternative blockchain that uses a more environmentally friendly method.

### 4.1 Ethereum standards

The first and most widely used token standard proposed by Ethereum is the ERC-20,<sup>4</sup> which supports only the creation of fungible tokens such as cryptocurrencies. However, it does not allow for the representation of non-fungible assets, and had thus to be modified to support the creation of the Cryptopunks.<sup>11</sup> In order to allow for interoperability in such applications, Ethereum later released its first NFT standard under ERC-721,<sup>5</sup> which was implemented in the CryptoKitties project<sup>17</sup> and has since become the dominant approach to implementing NFTs. This specification defines a minimum interface that a smart contract must adhere to in order to track and transfer NFTs. In particular, a unique token identifier is defined, which is the attribute that guarantees that every token is distinguishable from any other. The standard also leaves open the possibility to add metadata or supplemental functions.

Two notable alternative NFT standards on Ethereum are ERC-998<sup>28</sup> and ERC-1155.<sup>29</sup> ERC-998 compliant tokens are composable, which means that they can hold both unique non-fungible tokens (as in ERC-721), as well as uniform fungible tokens (such as ERC-20<sup>4</sup>). Since the ERC-998 token can own a unique set of digital assets, it can be thought of as a portfolio or as a holding company for a diverse set of assets. ERC-1155 tokens allow for users to register fungible and non-fungible tokens using the same address and smart contract. This token standard was developed for applications in gaming, where fungible tokens could represent a transaction currency in a game and non-fungible tokens could represent in-game collectibles and exchangeable assets.

### 4.2 Tezos standards

Tezos is a decentralized blockchain that uses the Proof of Stake<sup>8</sup> (PoS) consensus mechanism and relies on a native cryptocurrency called Tez. Tezos defines three primary token standards, of which only the FA2 is non-fungible. The FA2 token standard,<sup>30</sup> also known as the TZIP-12, is a unified token contract interface that supports a wide range of token types such as fungible, non-fungible, non-transferable and multi-asset contracts. It gives developers flexibility to define and to invent new token types which can support complex interactions while maintaining a standard API for external applications and wallets. These token structures can include NFTs and contain numerous different gaming items with interactive and transmutable features.

## 5. JPEG NFT INITIATIVE

Numerous digital assets used in NFTs are either in existing JPEG forms or in new and emerging JPEG formats. Additionally, several trust and security concerns have arisen regarding NFTs. JPEG standardization committee has a proven track record of ensuring the security and trustworthiness of imaging applications in addition to their efficient representation and coding. In light of this, the JPEG committee has launched a new exploration initiative focused on NFTs to determine how existing and emerging JPEG standardization activities in coding



and in system issues, can help increase the effectiveness and in particular the security and trust of NFTs in a wide variety of applications, particularly those that deal with digital assets that are represented by JPEG formats. The JPEG NFT initial steps include contacting stakeholders in NFTs and holding workshops to study NFT-related challenges and existing solutions, particularly in the context of applications relevant to the mandates of the JPEG standardization committee.

## 5.1 Scope of JPEG NFT

The JPEG Committee has defined the scope of JPEG NFT as:

The scope of JPEG NFT is the creation of effective specifications that support a wide range of applications relying on NFTs applied to media assets. The standard shall be secure, trustworthy and eco-friendly, allowing for an inter-operable ecosystem relying on NFT within a single application or across applications.

## 5.2 Current status of JPEG NFT

The JPEG Committee has been early to recognize the potential benefits of combining imaging with blockchain technology. Given that many digital assets in NFTs are in the form of contents (e.g., pictures, animations, 3D objects) that are readily represented in JPEG formats, it is a logical next step for JPEG Committee to explore opportunities for contributing to NFT standardization.

Much of JPEG's past and present activities relate to NFT-based media assets. These include: JPEG Universal Metadata Box Format (JUMBF), which allows embedding and referencing any metadata in any JPEG image; standardization efforts on Privacy and Security of JPEG Systems, intended to provide methods to protect metadata or (parts of) the image content; and the ongoing work on JPEG Fake Media, focused on the exploration of functions related to the creation of a standard that will facilitate secure and reliable annotation of media assets to combat malicious manipulation of genuine contents.

The current and near-term work of JPEG NFT exploration is to develop several use cases where JPEG can contribute with best practices and standards to solving techno-legal problems associated with NFTs and discussed in this paper. Towards this goal, stakeholders from academia, industry, and end-user communities have already participated in several workshops and will continue to participate in near-future workshops organized by JPEG.

The legal perspectives explored by JPEG NFT so far have included: NFT and its relation to certificate of authenticity; integration into NFTs of conditions of sale and use; the use of NFTs for legal monetization of physical artwork; compliance issues with financial and cryptocurrency laws in various jurisdictions; and legal issues with merchandising, transfer, and retraction rights.

JPEG NFT has explored the use case of NFTs by art marketers intending to understand the challenges associated with the beneficial use of NFTs in the art market. Of particular relevance to JPEG is the possibility of providing unique experiences to art collectors through the use of augmented and virtual reality headsets as well as future smart glasses. For example, the extensive efforts of JPEG Pleno, which aims to provide a standard framework for representing new imaging modalities (such as texture-plus-depth, light field, point cloud and holographic imaging), promise to enable NFT art collectors to enjoy realistic and interactive viewings of digital art in unprecedented ways.

## 6. CONCLUSION

In this paper we presented the concept and best practices of NFTs and the way they are implemented today. This allowed us to highlight a number of challenges that remain to be addressed in order to accelerate adoption of this new technology that some consider as the next revolution in the way assets in both digital and physical worlds are owned and exchanged. We then presented the current status of efforts undertaken by the JPEG standardization committee which is exploring creation of a new standard for NFTs that not only takes full advantage of the formats in which the digital assets are represented but also will allow to overcome other challenges highlighted in this paper, paving the road to NFT 2.0.

## ACKNOWLEDGMENTS

Fruitful discussions with several experts involved in the JPEG NFT initiative in form of brainstorming and exchange of information and opinion are hereby acknowledged. Authors from EPFL acknowledge support from MAKE, and interdisciplinary educational program from EPFL in the context of ProCam project.

## REFERENCES

- [1] Hripak, A., Arjona, S., Bohrer, J., Haag, V., Hata, T., Houston, C., Leuba, M., Miller, A., Mufeed, O., Otto, N., Pitcher, J., and Reis, A., *Open Badges Conformance and Certification Guide 2.1*. IMS Global Learning Consortium, Inc. (2020).
- [2] Nakamoto, S., “Bitcoin: A peer-to-peer electronic cash system.” <http://www.bitcoin.org/bitcoin.pdf> (2009).
- [3] Wood, G., “Ethereum: A secure decentralised generalised transaction ledger,” (2014).
- [4] Vogelsteller, F. and Buterin, V., *EIP-20: ERC-20 Token Standard*. Ethereum Improvement Proposals (November 2015). [Online serial]. Available: <https://eips.ethereum.org/EIPS/eip-20>.
- [5] Entriiken, W., Shirley, D., Evans, J., and Sachs, N., *EIP-721: ERC-721 Non-Fungible Token Standard*. Ethereum Improvement Proposals (January 2018). [Online serial]. Available: <https://eips.ethereum.org/EIPS/eip-721>.
- [6] Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., and Capkun, S., “On the security and performance of proof of work blockchains,” in *[Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security]*, *CCS ’16*, 3–16, Association for Computing Machinery, New York, NY, USA (2016).
- [7] Goodman, L., “Tezos — a self-amending crypto-ledger,” tech. rep. (2014).
- [8] Xiao, Y., Zhang, N., Lou, W., and Hou, Y., “A survey of distributed consensus protocols for blockchain networks,” *IEEE Communications Surveys & Tutorials* **22**, 1432–1465 (2020).
- [9] Szabo, N., “Smart contracts: building blocks for digital markets,” *EXTROPY: The Journal of Transhumanist Thought* (1996).
- [10] “Beeple’s opus: Created over 5,000 days by the groundbreaking artist, this monumental collage was the first purely digital artwork (nft) ever offered at christie’s.” <https://www.christies.com/features/Monumental-collage-by-Beeple-is-first-purely-digital-artwork-NFT-to-come-to-auction-11510-7.aspx> (Accessed at 25th July 2021) (2021).
- [11] “Cryptopunks.” <https://www.larvalabs.com/cryptopunks>.
- [12] “Cryptoslam.” <https://cryptoslam.io/> (Accessed at 25th July 2021).
- [13] “Nba top shot.” <https://nbatopshot.com/>.
- [14] “Bored ape yatch club.” <https://nbatopshot.com/>.
- [15] “The meebits.” <https://meebits.larvalabs.com/>.
- [16] “Axie infinity.” <https://axieinfinity.com/>.
- [17] “Cryptokitties.” <https://www.cryptokitties.co/>.
- [18] “Decentraland.” <https://decentraland.org/>.
- [19] “Nft license.” <https://www.niftylicense.org/> (Accessed at 26th July 2021).
- [20] “Bluebox.” <https://bluebox.info/> (Accessed at 26th July 2021).
- [21] “Ipfs.” <https://ipfs.io/>.
- [22] “Filecoin.” <https://filecoin.io/>.
- [23] “Arweave.” <https://www.arweave.org/>.
- [24] “Truffle.” <https://www.trufflesuite.com/truffle>.
- [25] “Hardhat.” <https://hardhat.org/>.
- [26] “Ganache.” <https://www.trufflesuite.com/ganache>.
- [27] “Openzeppelin.” <https://docs.openzeppelin.com/openzeppelin/>.
- [28] Lockyer, M., Mudge, N., and Schalm, J., *EIP-998: ERC-998 Composable Non-Fungible Token Standard [DRAFT]*. Ethereum Improvement Proposals (July 2018). [Online serial]. Available: <https://eips.ethereum.org/EIPS/eip-998>.

- [29] Radomski, W., Cooke, A., Castonguay, P., Therien, J., Binet, E., and Sandford, R., *EIP-1155: ERC-1155 Multi Token Standard*. Ethereum Improvement Proposals (June 2018). [Online serial]. Available: <https://eips.ethereum.org/EIPS/eip-1155>.
- [30] Mishura, E. and Mondet, S., “Fa2 - multi-asset interface.” <https://gitlab.com/tezos/tzip/-/blob/master/proposals/tzip-12/tzip-12.md> (accessed at 25th July 2021) (2020).