Oral communication: Towards mutable NFTs: Non-Fungible Mutable Tokens

Damiano Di Francesco Maesa*, Andrea Lisi*^, Paolo Mori^, Laura Ricci*, Simone Schiavone*
***University of Pisa, Pisa**
^Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche (CNR) , Pisa

Blockchain technology is a base component of the decentralised web, or Web 3.0, an evolution of Web 2.0 which pushes towards decentralisation of services and user self sovereignty. Users are no longer required to interact with centralised third party services for their digital needs, but they retain ownership and control over their own data and digital assets.

On the blockchain, digital assets are typically represented as tokens that, to date, follow two main models: fungible tokens and non-fungible tokens. Fungible tokens are interchangeable, meaning that each fungible token is identical to another token of the same family. Fungible tokens are suitable, for instance, to represent points on a loyalty card or coins. Non-Fungible tokens (NFTs) are non-interchangeable, meaning that tokens are unique and there exists only one token of that kind. Tokens are implemented by smart contracts on the blockchain tracking their owners and exposing the functions to regulate their transfer among users.

An envisioned usage of NFTs involves the metaverse, a digital world replicating the real one, its inhabitants, and their activities. NFTs can be used to represent on the blockchain the digital assets in the metaverse. An NFT's state typically contains a map of pairs, the identifier of the current asset owner, and the asset's unique reference. To ensure the reference is non-tamperable and unique, a cryptographic hash of the asset digital representation is often employed as reference. This model is simple and powerful enough for most use cases, but it has a major shortcoming. As the asset is represented on the blockchain by a non-invertible hash, all the asset characteristics are hidden behind it. Often the asset descriptor, whose hash is contained in the NFT, is stored off-chain that makes it difficult to be manipulated by on-chain entities (e.g. smart contracts). As a matter of fact, if the characteristics in the descriptor change, its hash changes as well and the NFT might need to be updated. This requires adopting workarounds, such as, for example, the destruction of the NFT and reissuing of a new one, with associated costs, or the inclusion of the mutable assets metadata to NFT contracts. This is evident with mutable assets, i.e., assets whose characteristics change as a normal consequence of their use. For example, assets that record the number of times they have been used. The asset characteristic "number of uses'' is an inherently dynamic one, ill suited for the static nature of NFT hashes.

We argue that digital assets should closely mirror real assets for the success of the metaverse. This includes supporting assets mutability, as most assets are dynamic in the real world.

In this oral communication we propose **Mutable NFTs** named **NMTs**, i.e. NFTs that keep the same asset reference independently of the underlying descriptor changes. Our proposed

NMTs support on-chain management of asset characteristics, enabling many use cases that would be impossible or overly complex with traditional NFT asset descriptors kept mainly off chain.

The NMT contract mirrors a traditional NFT contract, by following the same ERC 721 standard, but the linking of the NFT, i.e. the tokenURI, is the address of another smart contract: the asset contract for that given asset. Each asset will have its unique asset contract, while sharing the same NMT contract with all other assets of the same NMT class. The asset contracts would represent the descriptor of an asset, with its characteristics' values, the operations to update such characteristics, as well as the policies regulating the execution of such operations. This means that changes to said values are transparent and protected as intended as no value can be tampered with.

We showcase our concept of NMTs with a use case of a university in the metaverse. The university issues digital caps to its students as NFTs that the students can wear in the university's digital twin areas in the metaverse. Each cap is a mutable asset because it can be modified by inserting a pin for each exam the owner passes: a silver pin or a gold pin if the exam has been passed with honors. When a student graduates, the cap transforms into an academic hat. Figure 1 shows the graphical representation in the metaverse of a cap with no pins, with one pin, and with two pins.

Figure 1: Representation of the university cap in the metaverse

The state of a cap grants the students the rights to access to certain areas of the metaverse. For example, only the students with two pins on their caps can participate in the alumni exclusive event. The proof of concept has been developed with Solidity smart contracts that are invoked by a scene implemented in Decentraland.