Programmable NFTs and On-Chain Metadata: A Study

Anjani Gupta
Assistant Professor, Department of Information Technology
Dr. Akhilesh Das Gupta Institute of Technology and Management
New Delhi, India
anjaniaggarwal.06@gmail.com

Naman R Bhardwaj
Student, Department of Information Technology
Dr. Akhilesh Das Gupta Institute of Technology and Management
New Delhi, India
naman312010@gmail.com

Priyank Rastogi
Student, Department of Information Technology
Dr. Akhilesh Das Gupta Institute of Technology and Management
New Delhi, India
priyankrastogi14@gmail.com

Shubham Upreti
Student, Department of Information Technology
Dr. Akhilesh Das Gupta Institute of Technology and Management
New Delhi, India
shubham.upreti@gmail.com

***Abstract*—A Non-Fungible Token (NFT) is something that is not interchangeable with something else.It has its own unique identity and properties, much like a real life object. It can be a certificate, a painting, some music or a piece of virtual land. In practice, NFTs are simply packets of encapsulated data, with their state bound to the time of their creation. That is why their most popular implementation as of now is static media such as art, music, game tokens, utility like coupons, and so on. With this project, our aim is to bring NFTs closer to real life, and allow them to break out of the shell that is static properties. We intend to create NFTs whose properties can change as per the conditions provided by the creator of that NFT at the time of minting (creating) it. Through this method, The creator of that NFT can make it much closer to a real life object. A plant that can grow up, a virtual pet, a document that is supposed to expire and not exist after a certain period of time, a resource where access is supposed to stop after a certain period of time. This method is known to be much more expensive than the conventional method of storing just the Universal Resource Indicator (URI) in the smart contract, because blockchain is a ledger, and not intended as a database. The possibilities are only limited by imagination.**

***Keywords*—blockchain, NFT, metadata, trustless, mint, RPC, API, MATIC**

I. Introduction

The concept of non-fungible tokens has allowed blockchain technology to shine due to one of its core properties: immutability. Meaning, when someone makes an entry of their creation on a blockchain, its record stays there forever as a possession of that person until they change its ownership through the same blockchain.

Currently, the standards followed in the blockchain development industry pertaining to creation of NFTs render them uneditable, and this factor limits NFTs from showcasing the most important aspect of any real life object: the ability to change.

The current limitation with NFTs is that NFTs are absolutely uneditable. The method used as of now to create NFTs is that the metadata is compiled onto a single file, which is stored in turn on decentralized storage like IPFS (Interplanetary File System), and the unique link to this is in turn stored on the blockchain in a program by the method of a transaction. This creation transaction acts as a proof of ownership and so, an NFT is created. There is no way to change the properties of an NFT this way because if one were to tamper with the file uploaded to the IPFS, its hash would change, and as a result, the URI (Universal Resource Identifier) link to that file would change as well on the IPFS, with the link on the blockchain remaining the same as before, and thus, rendering it invalid.

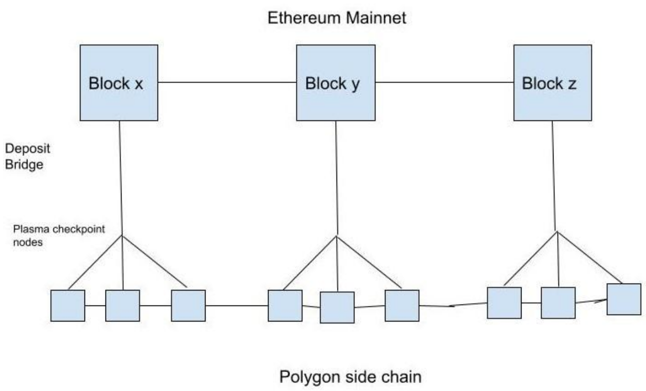
Through the methodology of keeping the NFT's metadata on the blockchain, we intend to store the metadata for each NFT in the smart contract in a defined object structure, so that we can cause its various properties to change with different kinds of interactions based on set parameters. This should allow us to make the NFTs programmable, i.e., to program certain behavior into NFTs so that their properties change reliably in a trustless environment, as should be the case with blockchain. This will be done by programming into the smart contracts extra effects when calling an 'update' function, for example.

Layer 2 blockchain solutions:

A layer 2 blockchain solution is a scalability solution for existing blockchains, which allow us to create our own sidechain or network of sidechains over a base chain. These layer 2 networks use the security and architecture of the base chain to ensure security and immutability.

Polygon[1] is a Plasma-based layer 2 solution, meaning multiple blockchains on the Polygon network can be created, which will all be interoperable. Over this Polygon network, they have released their own blockchain as well.

Image 1: Basic architecture of Polygon (previously MATIC)



Polygon blockchain is a newly released layer 2 blockchain solution, and through the study of its documentation and its transaction costs, we came to a conclusion that it would be possible to store metadata in smart contracts affordably, due to the transaction fees being extremely low when compared to Ethereum blockchain.

The next step would be to define some basic properties case-wise in the smart contract and program desired behavior in it using certain specialized functions. With this, the creator of the NFT would have a chance to define certain parameters for the NFT which would govern its behavior till its existence. Anything outside of this programmed behavior would not be supported by the NFT.

II. On-Chain Metadata

Metadata for NFTs is generally encapsulated in a JSON file, which in turn is uploaded on a hosted service (centralized or decentralized), and that link is recorded onto the blockchain, thus creating the NFT. The few advantages of this approach are:

- Low transaction fees when minting the NFT
- Metadata link does not change, thus pointing to the same resource.

Recently, there have been projects utilizing NFTs with editable metadata which is controlled by the creator, which brings along with it an unease as the parameters for change are controlled by the creator, which requires a degree of trust. Hence, these editable metadata NFTs are a risk to trade in as they are not very reliable. This environment warrants trust in the creator, which is against one of the core principles of decentralized technologies: trustlessness.

By storing metadata onto the blockchain and properly defining criteria for characteristics and modification, we create a trustless scenario, where the changes are occurring without direct intervention of the creator (or owner, in some cases). However, storing this much data, albeit not much, is a more expensive endeavor than just storing a URI (Unique Resource Identifier) to the metadata onto the blockchain. Thus, the downside of this approach is the increased transaction cost, or gas fees, incurred by the creator when actually making the NFT.

Do note, this methodology allows us to only create tailored solutions for particular kinds of NFTs. This means that following this train of thought, standard interactions and properties may be established for specific kinds of tokens needed. As an example, a multimedia file may have copies created of it, which carry an expiration time. When this time approaches, the transactions are blocked by the program to avoid further access and uses. In this way, multimedia can be reliably licensed.

Table 1: Price comparison between both methods and blockchains

Particulars	Ethereum	Polygon
Gas fees for minting as per standard	~0.0002 (Rs. 61.6)	~0.001 (Rs. 0.13)
Gas fees for minting while keeping metadata on-chain	~0.001 (Rs.305.07)	~0.01 (Rs. 1.36)

Storing metadata on-chain allows us to program various changes in the various reading and transfer functions of the smart contract so that we can introduce a change with every desired action on/of the NFT.

As an example, an NFT with an expiration time would have checks programmed into its reading and writing functions to check the expiration time. When it expires, then it is destroyed in the smart contract. This methodology ensures that the token does not live past its defined lifetime.

Having on-chain metadata also may allow us to grant provenance to the metadata, since the changes themselves would be visible in the blockchain's transaction records.

III. Programmable NFTs

Considering we have the metadata for NFT on the blockchain encoded as a JSON, we can implement various structures, functions and restrictions as per the particular case where this methodology needs to be applied. However, on a blockchain, there always needs to be a call to a function for it to trigger, that is, that there is no method to automate changes, and so conditions need to be applied to various functions to enable the NFT to change its properties.

For example, upon every subsequent transfer, an NFT changes its appearance, like a piece of cloth getting worn out, or an article of glass cracking with use. An NFT plant may grow to be a tree in this way.

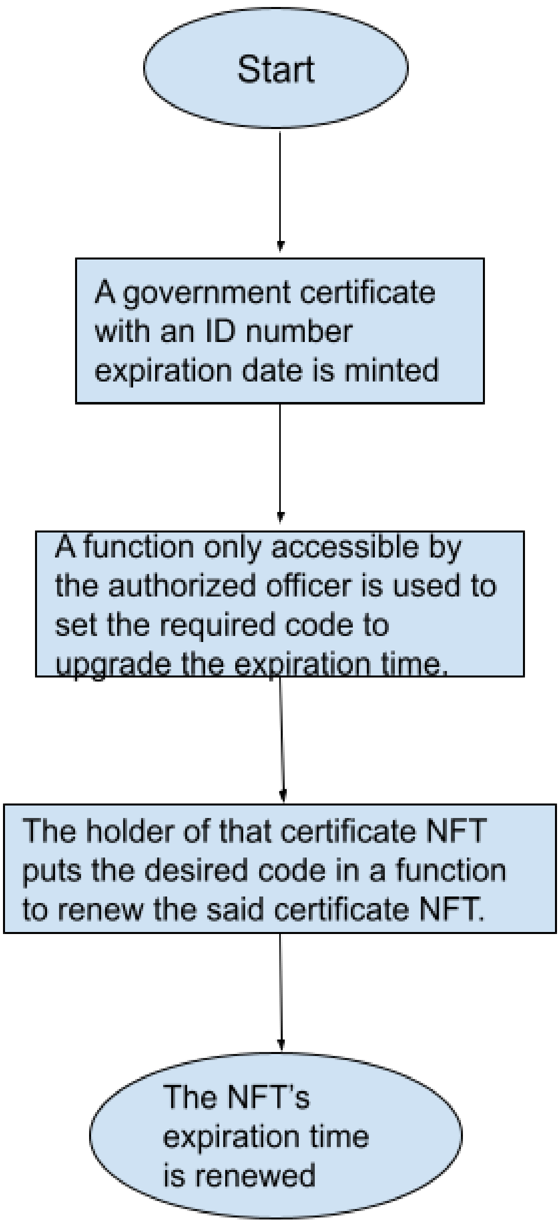
The downside of this methodology is that this is not a general solution. Meaning, depending on the use case of a particular kind of NFT, the programmable fields' properties and expectations may change. This cannot be applied feasibly as a general solution as like real life objects, NFTs of various types will have their own properties to obey. A piece of jewelry cannot behave like a hammer or vice versa, and so on and so forth. However, the nature of blockchain being immutable, transparent and decentralized makes it a good idea to invest in such varied solutions anyway.

Since a program needs to be deployed only once to be able to interact with it forever, along with this comes the guarantee of safekeeping of the data of tokens along with guaranteeing their existence (at a point of time) along with their whole history being available at all times.

Therefore, not only does on-chain metadata allow for regulating media and information, it also guarantees that none of the parties involved would face unfairness. Just like an NFT with an expiration date may expire at some time, it is also guaranteed that the NFT will not expire before that time, no matter the wishes of the parties concerned with that NFT.

An implemented and tested example is as follows:

Image 2: The flow of an implemented example



As it is seen, this method allows for secure metadata modification through the blockchain, creating a trustless environment where the NFT can change without malicious parties being able to interfere.

This also proves that by creating some flexibility in how metadata is handled, the utility of NFTs increases by many-fold.

IV. Change in Metadata and Metadata Provenance

Allowing the functionality for change in metadata does not mean that older data will be lost forever. Since the transaction data of the blockchain would forever be visible, changes in data can be detected and recorded by indexing and archiving the said data. Using this, the various versions of the NFT metadata can be maintained off-chain.

To maintain all metadata versions on the chain inside the program, however, would be an expensive endeavor and would not yield much usefulness.

Metadata provenance is an important factor that lends to the legitimacy of the token and blockchain, allowing it to be the primary reason that we are able to support such complex life-like tokens on this platform.

V. Result and Discussion

The provable applications of this project are, but not limited to:

1. NFTs that can age: This would allow for verified documents that can expire or art that changes appearance or NFTs whose access needs to be stopped at a later time.

   Eg: A virtual bronze sculpture that can age, licensed media whose access should be stopped after certain time, or certificates with a limit to validity

2. NFTs that change properties: NFTs that change properties based on who it is owned by, or perhaps which NFTs are in their possession

   Eg: A document whose expiration time gets pushed when an NFT carrying a particular message in its data comes in the possession of the user, or an NFT changes some property according to the end character of the public address of the ownership

The disadvantages of this approach entail:

1. This is not a generalized solution for creating NFTs. This is because every object has different properties and thus the handling of

various kinds of objects must be dealt with in various corresponding methods.
2. This approach will not currently be supported everywhere due to present solutions being tailored for static NFTs.
3. The programming skill required for such an approach's implementation is higher and more dynamic than current standards.
4. The increase in transaction costs due to this approach may not be much for an individual when using Polygon. However, when viewed with reference to the huge volumes of NFT creation, this will cost an astronomical amount when looked at by volume, when compared with traditional methods.
5. This is impractical for blockchains that have much higher transaction fees.

The advantages for this approach are:
1. NFTs can become programmable and more lifelike. This will equate to true utility and usability, rather than just being expensive art pieces.
2. The programmability will make it possible to transfer real-life things' records onto the blockchain, making them permanent and immune to loss, saving unreal amounts of assets for users, often caused by proofs of ownership or going missing.

VI. Future Scope

While the NFT market is already worth millions of US Dollars, its utility is negligible to what it could be if we implement programmability in NFTs. This method, albeit present, is scarcely used due to the endless number of cases and lack of a method of generalization. However, this approach of keeping metadata on-chain for tokens is expanding in use with the advent of multitudes of use cases of blockchain finding its way into the industry.

The adaptation of this approach could change the way we prove legitimacy and properties of an object to others, as the records would be permanent on the blockchain, including the various versions of an object that have ever existed. This would pave the way to almost all real objects being bound to fungible or non-fungible token counterparts onto the blockchain.

The rapid developments in the blockchain technology will most definitely accommodate the need fo dynamit tokens which correspond to all real objects. This wave of programmable NFTs is set to start with simple artworks, but will surely develop into something grandiose with the acceptance of the blockchain technology.

References

[1] Polygon documentation: https://docs.polygon.technology/docs/home/new-to-polygon

[2] Ethereum NFT standard: https://eips.ethereum.org/EIPS/eip-721

[3] A conceptual model for Indian public distribution system using consortium blockchain with on-chain and off-chain trusted data Sandeep Kumar Singh, Mamata Jenamani, Diptiman Dasgupta & Suman Das

[4] Chmarusso's SwordNFT.sol https://gist.github.com/Chmarusso/045ee79fa9a1fae55928a613044c9067

[5] Demichev, Andrey & Kryukov, Alexander & Prikhod'ko, Nikolay. (2018). The Approach to Managing Provenance Metadata and Data Access Rights in Distributed Storage Using the Hyperledger Blockchain Platform.

[6] Barriocanal, Elena & Sánchez-Alonso, Salvador & Sicilia, M.. (2017). Deploying Metadata on Blockchain Technologies. 38-49. 10.1007/978-3-319-70863-8_4.

[7] Faisal, Tooba & Courtois, Nicolas & Serguieva, Antoaneta. (2018). The Evolution of Embedding Metadata in Blockchain Transactions. 1-9. 10.1109/IJCNN.2018.8489377.

[8] Bhama, Ponsy & Jayabal, Chandra. (2021). MetaInfoChain: Bi‐layered blockchain consensus for metadata aggregation in IoT and cloud environments. Transactions on Emerging Telecommunications Technologies. 32. 10.1002/ett.4362.

[9] Zhang, Lejun & Zeng, Weimin & Jin, Zilong & Su, Yansen & Chen, Huiling. (2021). A Research on Traceability Technology of Agricultural Products Supply Chain Based on Blockchain and IPFS. Security and Communication Networks. 2021. 1-12. 10.1155/2021/3298514.

[10] Schardong, Frederico & Custódio, Ricardo & Pioli, Láercio & Meyer, João. (2022). Matching Metadata on Blockchain for Self-Sovereign Identity. 10.1007/978-3-030-94343-1_32.

[11] Kolydas, Tassos. (2019). Timestamping Metadata Using Blockchain: A Practical Approach. 10.1007/978-3-030-36599-8_42.

[12] Kate Hertz. Know the Difference: On-Chain and Off-Chain NFTs - https://www.one37pm.com/nft/tech/on-chain-and-off-chain-nfts

[13] Nicola Attico. ERC-721 Token with on chain metadata- https://nicola-attico.medium.com/erc-721-token-with-on-chain-metadata-d5e9527102cc