AINFTs: Reproducible Generative NFTs

Basil Roy
http://ainft.website

September 24, 2024

Abstract

Non-Fungible Tokens (NFTs) have revolutionized the collection and trading of digital assets on blockchain platforms. However, a significant limitation of traditional NFTs is that the digital assets they represent are not stored directly on the blockchain. Instead, they typically reference external resources, which can lead to potential loss or inaccessibility of the asset if the external source becomes unavailable. This paper introduces AINFTs, a novel approach that addresses this vulnerability. Rather than storing a URL pointer, AINFTs encode a seed for a data generation model within the blockchain itself. This method ensures that even if the original asset becomes inaccessible, it can be faithfully regenerated using the on-chain seed and an associated open-source off-chain generation model, thus preserving the NFT's value and integrity indefinitely.

1 Introduction and Overview

Non-Fungible Tokens (NFTs) are a revolutionary paradigm in digital asset ownership. By leveraging distributed blockchain technology, NFTs establish a decentralized ownership record system that operates independently of any central governing authority. This innovative approach has catalyzed a surge in popularity, attracting both collectors and artists to the technology in unprecedented numbers. However, the current implementation of NFTs is not without fundamental problems.

First, the implementation of most NFTs does not actually store the digital asset on the blockchain. This is due to the typically large file sizes of digital assets, which make it inefficient and economically impractical to store them directly on the blockchain. Instead, NFTs generally store a Uniform Resource Identifier (URI) that points to the location of the actual digital asset. These assets are typically stored on the internet and accessed via protocols such as HTTP or IPFS (InterPlanetary File System).

This approach presents a significant limitation: the actual digital asset is not intrinsically linked to the on-chain NFT. The digital asset referenced by the URI could potentially become inaccessible or be altered without affecting the NFT itself. While distributed protocols such as IPFS [1] and Arweave [9] offer partial solutions to this issue, they are not without their own limitations. IPFS, for instance, utilizes content-based addressing with immutable URIs derived from data hashes. However, IPFS files require continuous "pinning" to ensure their persistence on the network, and there remains a possibility of permanent data loss if a file is not adequately maintained. Arweave presents a more robust solution with its pay-once, store-for-200-years model, but even this impressive duration falls short of true permanence.

The second limitation of traditional NFTs concerns their uniqueness and provability. There is no inherent mechanism to prevent the duplication of asset data and the subsequent creation of a new NFT with identical content. This vulnerability undermines the fundamental premise of NFTs: unique digital ownership. Consequently, this has led to a proliferation of counterfeit NFT scams [3]. To illustrate the magnitude of this issue, OpenSea, a prominent NFT marketplace, reported that 80% of NFTs created using their tool "were plagiarized works, fake collections, and spam" [5]. This statistic underscores the severity of the problem and the urgent need for more robust authentication mechanisms in the NFT space.

To address these issues, we introduce a novel concept called "AINFTs." Unlike traditional NFTs, an AINFT does not store a link to a digital asset. Instead, it encodes a seed within the blockchain that is used to generate the digital asset. This seed, combined with a publicly available generation model, allows for the complete reconstruction of the digital asset without any loss of data. The immutability of the blockchain ensures that the seed cannot be removed or modified, thus preserving the AINFT indefinitely.

The process of generating a human-viewable image from a AINFT occurs off-chain, utilizing an open-source image generation model. This approach enables anyone with access to the generation model to reconstruct any AINFT. Moreover, the public nature of the seeds facilitates easy verification of a AINFT's authenticity. Any interested party can generate the image associated with a AINFT using the public seed, thereby confirming its content.

The AINFT system allows for a vast number of mints, up to $2^{63} - 1$, corresponding to the range of possible seeds in the image generation model. To support the infrastructure necessary for integration with traditional NFT platforms such as OpenSea, the project administrators impose a nominal minting fee. This fee facilitates the automatic generation and hosting of images, enabling AINFTs to be seamlessly traded on established NFT marketplaces. It is important to note that while this hosting service enhances the user experience and reduces adoption barriers, it is not fundamentally necessary for the AINFT system. The images can be independently regenerated by any party with access to the public seed and generation model. The project reserves the right to adjust the minting fee to maintain the value proposition for existing AINFT holders and ensure the long-term sustainability of the project.

The minting process of AINFTs introduces an element of unpredictability and excitement. Each minted token generates a unique image, the quality and appeal of which cannot be predetermined. This inherent variability in outcomes adds an engaging aspect to the minting experience. Users may obtain a range of results, from aesthetically pleasing to less desirable images, all of which are revealed only after the minting process is complete. We believe this element of surprise and discovery will contribute significantly to the appeal and adoption of AINFTs.

While generative NFTs, such as Art Blocks' Chromie Squiggles [2], already exist in the market, AINFTs offer several distinct advantages. Firstly, traditional generative NFTs are often limited in their supply, typically ranging from hundreds to thousands of tokens. In contrast, AINFTs have the capacity to mint an unprecedented $2^{63} - 1$ unique tokens, providing a vastly larger pool of potential assets.

Secondly, existing generative NFTs frequently rely on relatively simple geometric concepts or algorithmic patterns that can be encoded in basic computer programs. AINFTs, however, leverage advanced diffusion image generation models, resulting in a significantly more diverse and aesthetically sophisticated output. This approach allows for the creation of complex, varied, and visually appealing images that go beyond the constraints of traditional

generative art algorithms.

The combination of these factors - the expansive minting capacity and the utilization of state-of-the-art image generation techniques - positions AINFTs as a notable advancement in the field of generative NFTs, offering enhanced scalability and artistic diversity.

2 AINFT Smart Contract

AINFT is implemented as an ERC721A contract[4], a choice motivated by its gas-efficient minting process for multiple NFTs. This efficiency is particularly advantageous for AINFT, as we anticipate users will be inclined to mint multiple tokens. The ERC721A standard allows for this without incurring prohibitively high gas fees.

The primary modification to the ERC721A standard in our implementation involves the calculation of a seed during the minting process, which is subsequently utilized for image generation. This seed is derived using the Keccak-256 hash function, with inputs comprising the block number, block timestamp, sender address, and NFT ID. In cases where multiple tokens are minted in a single transaction, the first token's seed is generated using the hash function, while the seeds for subsequent tokens are incremented from this initial value. This approach is designed to maintain compatibility with ERC721A's mechanism for efficient minting of multiple tokens simultaneously.

While the seed generation process is not entirely random, it provides a sufficient level of unpredictability for the intended purpose. A determined user could theoretically predict the inputs of the Keccak algorithm and preview the resulting image before minting the NFT. This could potentially allow for selective minting, where users choose to mint only aesthetically pleasing images. However, in practice, this does not pose a significant limitation to the system's integrity for several reasons:

1. Temporal constraints: The components of the random algorithm (e.g., block number and NFT ID) are likely to change during the time it takes to generate and assess an image, rendering any prediction attempts difficult.

2. Computational intensity: Continuously generating and assessing images before minting would be both time-consuming and computationally intensive, likely outweighing any potential benefits.

3. Economic disincentive: The cost and effort required for such an approach are likely to exceed any potential gains, thus discouraging users from attempting to game the system.

4. Irreversibility of Keccak: The Keccak hash function is not reversible, making it impossible to work backwards from a desired seed to determine the inputs needed to create that seed.

Given these factors, we have determined that the current seed generation method provides an adequate balance between randomness and efficiency, without the need for an external randomness oracle. This approach maintains the integrity of the AINFT system while ensuring a fair and engaging minting process for all users.

AINFT is deployed on the Polygon chain, to reduce gas fees. The contract can be viewed at `https://polygonscan.com/address/0xaF63754FFDCCEFd9d18cF3e1dd96FD013572164a`.

3 AINFT Image generation

The state-of-the-art image generation models are predominantly based on diffusion techniques. For our implementation, we employ a high-speed diffusion model, specifically SDXS-512-DreamShaper, to generate images [7]. While this model may not produce the highest image quality available, its exceptional speed allows for efficient minting of a vast number of NFTs. This trade-off between quality and speed is crucial for the scalability of our AINFT system.

The image generation process requires a text prompt that describes the desired content of the image. To generate these prompts, we developed and trained a specialized prompt generation model. This model is designed to produce a diverse array of unique prompts, ensuring a wide variety of generated images. For this purpose, we employed a compact language model based on the GPT-2 architecture [6], comprising approximately 124 million parameters. The relatively modest size of this model is sufficient for our needs, as the task of generating image prompts is comparatively straightforward and does not necessitate the complexity of larger language models. This approach allows us to maintain efficiency while still achieving the desired diversity in prompt generation. In Figure 1 we show the first 16 AINFTs minted using our method.

While the prompt generation model is designed to produce diverse outputs, it is important to note that absolute uniqueness of prompts cannot be guaranteed. There exists a possibility, albeit small, that a limited number of AINFTs may generate identical prompts, even with different seeds. To evaluate the effectiveness of our prompt generation model in producing unique outputs, we conducted an empirical analysis. We generated a sample of 100,000 prompts and found only 45 prompts were not unique. In this rare case, the generated image will be similar but not the same because the seed will also affect the output of the image generation model. The likelihood of an identical prompt with an identical image is extremely low, although we did not simulate this probability due to computational resources.

To facilitate the verification of NFTs, we have made both the model weights and the inference code publicly available in our GitHub repository[1]. This transparency allows users and developers to independently verify the authenticity and generation process of our AINFTs.

Ensuring consistent image generation across different systems is crucial for the integrity of our AINFT implementation. However, achieving this consistency presents challenges due to variations in neural network library implementations. In our implementation, we have taken several measures to maximize consistency:

1. We have fixed the versions of PyTorch and all associated libraries to ensure a stable environment.
2. We explicitly force the model to operate on the CPU to avoid GPU-related inconsistencies.
3. We discovered that PyTorch's multinomial function produced inconsistent results across different CPU architectures. To mitigate this, we reimplemented the network's decoding function using a custom multinomial function.

Despite these efforts, minor discrepancies may still occur in the final image output due to differences in neural network operations across CPU architectures. These differences

[1] `https://github.com/basilroy76/AINFT`

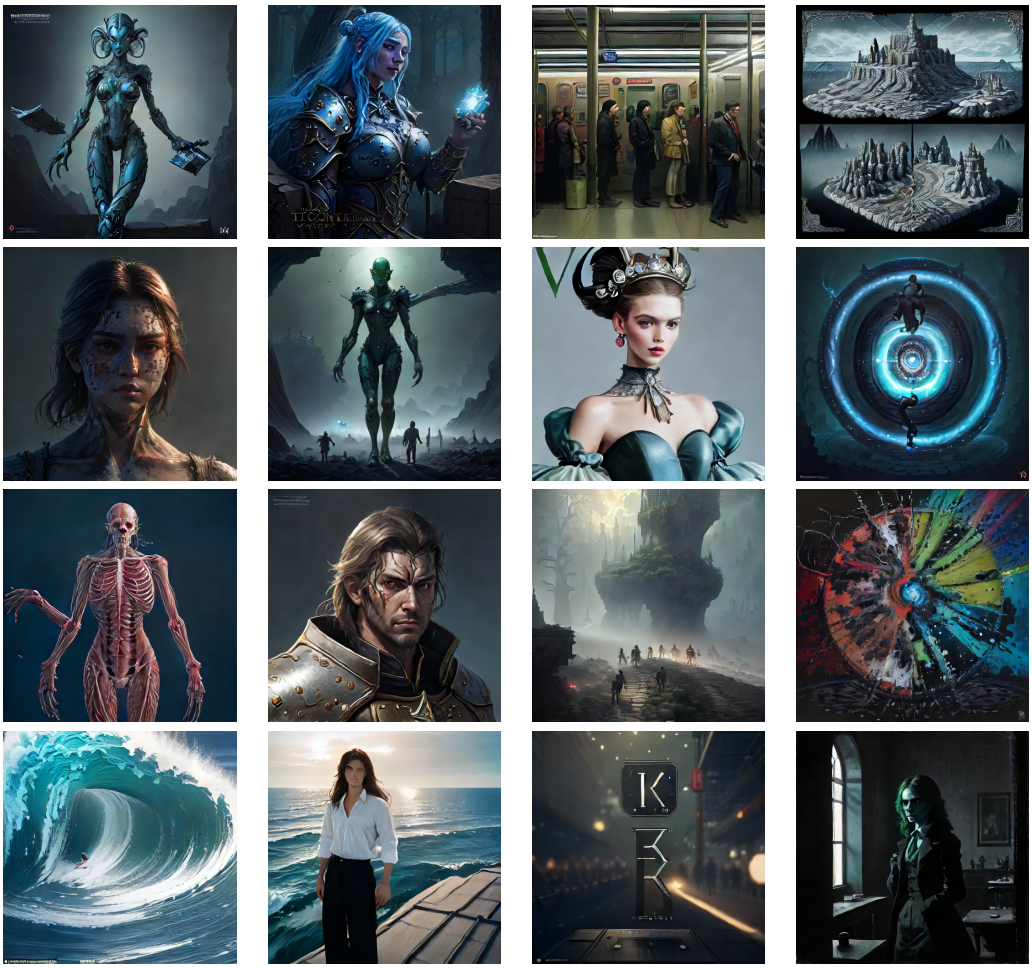

Figure 1: The first 16 generated AINFTs.

typically result in a Mean Squared Error (MSE) of 0.02 or less between images generated on different systems. However, these variations are imperceptible to the human eye and do not significantly impact the visual quality or uniqueness of the generated images. Therefore, we consider these minor differences acceptable within the context of our AINFT system.

4 AINFT Integration into NFT marketplaces

While the aforementioned code can be utilized to independently generate images for tokens, we have implemented additional infrastructure to facilitate the integration of AINFTs into existing NFT marketplaces. This integration is crucial for promoting widespread adoption and accessibility of our AINFT system.

Existing NFT marketplaces require that images and metadata be stored in a specific location. To facilitate this, we have developed a streamlined system that monitors blockchain events for generation triggers, subsequently produces the images and associated metadata, and finally notifies OpenSea to refresh the metadata. It is important to note that this process is not instantaneous, particularly when multiple NFTs are minted simultaneously. Consequently, there may be a delay before the images appear on the marketplace. Users should be aware of this potential lag and not be concerned if their images do not manifest immediately upon minting.

The metadata comprises essential information, including the unique identifier (ID) of the minted NFT and the corresponding random seed. This configuration enables users on platforms like OpenSea to verify the authenticity of the NFT using only the metadata, without the need for direct blockchain interaction. Looking ahead, there is potential for NFT marketplaces to integrate native support for generative NFTs. In such a scenario, the marketplace itself could generate the NFT on-demand, thereby ensuring its authenticity and providing an additional layer of verification for users.

5 Limitations

While AINFTs offer significant improvements in addressing the authenticity challenges associated with traditional NFTs, they do not entirely eliminate these issues. It remains possible for individuals to replicate images from popular generative NFTs and create duplicate traditional NFTs using these copied images. However, the verifiable nature of generative NFTs provides a potential solution to this problem. We believe that through comprehensive user education and the promotion of verification practices, the authenticity of AINFTs can be effectively maintained and distinguished from unauthorized duplicates.

Similarly, there exists a potential vulnerability wherein an individual could replicate an existing AINFT project and deploy it to the blockchain under a different address. Given that the generation seeds are publicly accessible, a malicious actor could program their cloned NFT to reproduce the seeds from the original project. In this scenario, the generative NFT verification process would succeed, potentially misleading users into purchasing counterfeit NFTs. Therefore, it is imperative for users to verify both the contract address and the NFT itself. To mitigate this risk, the development of trusted automated tools that simultaneously authenticate both the contract address and the generated asset could prove beneficial in enhancing security and user protection.

From an artistic perspective, the AINFT system has certain limitations due to the relatively small size of the diffusion model employed. This constraint results in inconsistent

quality across the generated images. However, this inconsistency inadvertently introduces an intriguing dynamic to the system. Some minted NFTs may be of lower quality, potentially limiting their resale value, while others may exhibit exceptionally high quality. This variability creates a collection experience reminiscent of opening a pack of collectible trading cards. The element of unpredictability in image quality adds an engaging aspect to the AINFT ecosystem, potentially encouraging users to participate in the "collection" process.

5.1 Duplicate Seeds

An important limitation of the seed generation technique is that seeds are not guaranteed to be unique, as we do not generate them sequentially. This design choice is intentional to prevent users from predicting the resulting image before minting. Consequently, there exists a non-zero probability that duplicate seeds may be minted.

To address this limitation, we can compute the probability of duplicate seeds occurring. Let us assume a scenario with 1 million mints, where each mint generates a single seed. The total number of possible seeds is $2^{63} - 1$. Given these parameters, we can estimate the probability of a collision using the well-established result from the birthday problem in probability theory [8].

The probability of at least one collision in n trials, where each trial selects from m possibilities, can be approximated using the following formula:

$$P(\text{at least one collision}) \approx 1 - e^{-\frac{n^2}{2m}}$$

In our case, $n = 1,000,000$ (number of mints) and $m = 2^{63} - 1$ (number of possible seeds). Substituting these values:

$$P(\text{at least one collision}) \approx 1 - e^{-\frac{1,000,000^2}{2(2^{63}-1)}}$$

This calculation yields a probability of approximately 5.4×10^{-8}. This extremely low probability indicates that the chance of a duplicate seed occurring is negligible, though not impossible. Given the extremely low probability of duplicate seeds occurring, we have decided to proceed with the current implementation, acknowledging this limitation.

6 Conclusion

This paper introduces AINFTs. AINFTs address several critical shortcomings of traditional NFTs by embedding a seed for a data generation model directly into the blockchain. This approach not only guarantees the enduring preservation of digital assets, but also enables their authenticity to be easily verified. Future AINFTs could be expanded to other modalities, or artists could carefully curate a diffusion model to produce NFTs with desired artistic qualities. AINFTs can be minted on our website at `http://ainft.website`.

References

[1] Juan Benet. Ipfs-content addressed, versioned, p2p file system. *arXiv preprint arXiv:1407.3561*, 2014.

[2] Art Blocks. Chromie squiggle by snowfro. https://chromie-squiggles.com, 2021. Accessed: 2024-09-16.

[3] Dipanjan Das, Priyanka Bose, Nicola Ruaro, Christopher Kruegel, and Giovanni Vigna. Understanding security issues in the nft ecosystem. In *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security*, pages 667–681, 2022.

[4] Chiru Labs. Erc721a. https://github.com/chiru-labs/ERC721A, 2022. Accessed: 2024-09-16.

[5] OpenSea. Tweet on fake nfts. https://x.com/opensea/status/1486843204062236676, 2022. Accessed: 2024-09-16.

[6] Alec Radford, Jeffrey Wu, Rewon Child, David Luan, Dario Amodei, Ilya Sutskever, et al. Language models are unsupervised multitask learners. *OpenAI blog*, 1(8):9, 2019.

[7] Yuda Song, Zehao Sun, and Xuanwu Yin. Sdxs: Real-time one-step latent diffusion models with image conditions. *arXiv preprint arXiv:2403.16627*, 2024.

[8] Wikipedia contributors. Birthday problem — Wikipedia, the free encyclopedia. https://en.wikipedia.org/w/index.php?title=Birthday_problem&oldid=1247519966, 2024. [Online; accessed 25-September-2024].

[9] Sam Williams, Viktor Diordiiev, Lev Berman, and Ivan Uemlianin. Arweave: A protocol for economically sustainable information permanence. *Arweave Yellow Paper*, 2019.