Non-Fungible Tokens for Confidential Assets

Pierpaolo Della Monica[2], Ivan Visconti[1], Andrea Vitaletti[2], and Marco Zecchini[1]

[1] University of Salerno, Fisciano, Italy
{visconti, mzecchini}@unisa.it
[2] Sapienza University of Roma, Rome, Italy
{dellamonica, vitaletti}@diag.uniroma1.it

For centuries people have enjoyed owning expensive objects (e.g., jewelry, expensive cars, paintings), often to show off their power and their wealth. Such expensive objects gain their value because they are available in a limited quantity and other people strongly desire to have or use them. By owning such objects we mean that the owner has exclusive access to them and the permanent or temporary transfer of such ownership fuels a relevant business activity.

In the digital world, "objects" are modeled by files. Every file is replicable, and data replication is often highly recommended (e.g., backups). Hence, the concept of scarcity has shifted from the file itself to its ownership. In other words, since it is hard to guarantee that a single copy of a file exists, there is a general goal aiming at guaranteeing that at each instant in time, only one legit owner of the file exists and the only way a copy of the original file can circulate is because the owners (either the current or the past ones) disclose it. Moreover, there should exist mechanisms allowing the transfer of ownership, keeping confidential the file so that only the old owners and the new one will have access to the original file.

The way such a trade of a confidential file is nowadays conducted, however, is not satisfying. In traditional client/server applications, users *trust* an intermediary for storing a digital file and for implementing access-control policies to limit exposed information of the stored files (i.e., previews) and fairly trade a file either to sell a copy of the file or to transfer its ownership. Notably, there is a flourish market of web services selling high-resolution images over the Internet (e.g., Getty Images, [1] Shutter Stock and Deposit Photos) that work as follows: first, the owner of an image uploads it to the web service, which then generates a low-quality version of the image and makes this new version publicly accessible; then, the original image is kept private and is disclosed only to users who have completed a payment for getting access to it.

However, trusted third parties (TTPs) are potentially vulnerable to corruption and moreover they could be successfully attacked becoming unreliable against their will (e.g., images deposited in a TTP could be stolen in case of a data breach). Moreover, a mediator that is considered reliable, is usually expensive. Hence, it is preferable to avoid designs that strongly rely on TTPs.

With the advent of blockchain technology, peers achieve consensus on the system status without relying on TTPs. This technology crucially enables a new form of decentralized trading for files and this is achieved by associating files to tokens, and establishing token ownership and transfer mechanisms. Such tokens are not interchangeable, as regular currency, because two distinct tokens represent two distinct files. For this reason, these specific tokens are called Non-Fungible Tokens (NFTs). The NFT trading is typically managed by a smart contract, which is a program running on the blockchain. The decentralized nature of smart contracts enhances the security of the trading system because it does not rely anymore on a single entity but on the security of the underlying blockchain technology. Such security, among other features, relies on transparency, namely the possibility for any user to autonomously verify that the status of the system is correct by accessing all its data (e.g., scanning all blocks of the ledger, all transactions included in them, and accessing files associated with NFTs on decentralized storage platforms as IPFS). However, transparency affects negatively the confidentiality of an asset. Obviously, through classical encryption techniques, an owner can obfuscate the file associated with an NFT. However, in this way, it becomes difficult for the owner to advertise her asset. Moreover, when a file is encrypted one needs to ensure that after a valid payment from the buyer, the seller discloses the key used to encrypt the file. If the key is not correct, the buyer should compute a proof of misbehavior of the seller

[1] The revenue value of the only Getty Images service in 2023 is over 225 million dollars.

and could complain to a "judge" (that on blockchain applications is a smart contract) getting a full refund for its payment. At the same time, the seller that delivers the wrong key should be financially penalized by the judge (i.e., the smart contract). This fair trade of a special information (i.e., the encryption key in our case) has been explored in the literature [1, 4]. All these studies take for granted that the buyer and the seller set an off-chain communication channel to exchange the necessary messages to complete the sale successfully. Hence, users must rely on external services that can be either single points of failure in a decentralized architecture, or difficult to implement for non-advanced users.

Open Problem. Motivated by the above considerations, the main question addressed by our work concerns the possibility of designing a system for the management of NFTs, in which owners of digital assets (e.g., art sellers) can autonomously advertise their assets by publishing preview versions and monetizing them through the blockchain, with an NFT transfer mechanism that allows an owner to transfer the ownership and guarantees both buyer and seller all the desired security and privacy properties. For the sake of simplicity, we will focus on the sale of images, and to support this vision in a decentralized environment, we require a mechanism to guarantee the correct purchase/exchange of confidential high-resolution images that are advertised only through previews decided by their owners.

Our Results

In this work, we address the aforementioned problem by introducing a new type of token called Confidential Non-Fungible Token (CNFT). This token inherits all the features of a standard NFT, enabling the regulation of digital asset ownership through decentralized platforms, and enhancing its functionalities. A CNFT does not permit public access to the corresponding digital asset, providing only an authentic preview of original data, and it ensures the existence of an encrypted high-resolution version of the data for which the CNFT owner possesses the decryption key. Furthermore, the CNFT enables a protocol for the secure exchange of the decryption key over a blockchain ensuring that the seller cannot be paid without providing the decryption key to the buyer, and the buyer cannot obtain the decryption key without paying the seller.

We have designed a system that guarantees that a) a ciphertext corresponds to the encryption of an authenticated image (e.g., an image digitally signed by its author) through a symmetric encryption scheme, and b) a committed message corresponds to the secret key used for the encryption. Both the ciphertext and the transformed image, along with the commitment of the secret key, are public and attached to the CNFT.

Furthermore we have designed a secure exchange of the secret key on the blockchain within a smart contract that acts as an intermediary between the two parties, the seller and the buyer.

We have evaluated the performance of our implementation on different images, aligning with the most prominent (in terms of market capitalization) NFT collections[2]. Our approach turns out to be compatible with all existing collections and also suitable for larger images.

Ensuring transformation integrity with proofs. A tool that we will crucially need is a mechanism to ensure that an image has been correctly transformed according to public specifications. Starting with the foundational work of [6], known results of [2, 5] show how to exploit special zero-knowledge (ZK) proofs named ZK-snarks to guarantee that some specific transformations have been applied to an authentic original image. Results of [2, 5] require very expensive hardware. More recently, the work of [3] introduces a novel mechanism for enabling a practical proof computation (i.e., achievable on a common laptop) to guarantee that a specific set of transformations has been applied to an original image. In [3], the authors demonstrate that their system preserves the confidentiality of the original image while ensuring the authenticity of the low-quality version. Additionally, they highlight that the proofs are easily computable even on a standard laptop. Moreover, their system offers a very efficient mechanism to verify fraud proofs.

[2] https://ebutemetaverse.com/nft-image-size

References

[1] Matteo Campanelli, Rosario Gennaro, Steven Goldfeder, and Luca Nizzardo. Zero-knowledge contingent payments revisited: Attacks and payments for services. In Bhavani M. Thuraisingham, David Evans, Tal Malkin, and Dongyan Xu, editors, *ACM CCS 2017*, pages 229–243. ACM Press, October / November 2017. doi:10.1145/3133956.3134060.

[2] Trisha Datta and Dan Boneh. Using zk-proofs to fight disinformation. In *Real World Crypto (RWC)*, 2023. URL: https://rwc.iacr.org/2023/acceptedpapers.php.

[3] Pierpaolo Della Monica, Ivan Visconti, Andrea Vitaletti, and Marco Zecchini. Detecting disinformation through cryptography, 2024. ITASEC 2024 submission. Accept at IACR Real World Crypto Symposium 2024.

[4] Stefan Dziembowski, Lisa Eckey, and Sebastian Faust. FairSwap: How to fairly exchange digital goods. In David Lie, Mohammad Mannan, Michael Backes, and XiaoFeng Wang, editors, *ACM CCS 2018*, pages 967–984. ACM Press, October 2018. doi:10.1145/3243734.3243857.

[5] Daniel Kang, Tatsunori Hashimoto, Ion Stoica, and Yi Sun. Zk-img: Attested images via zero-knowledge proofs to fight disinformation, 2022. doi:10.48550/ARXIV.2211.04775.

[6] Assa Naveh and Eran Tromer. PhotoProof: Cryptographic image authentication for any set of permissible transformations. In *2016 IEEE Symposium on Security and Privacy*, pages 255–271. IEEE Computer Society Press, May 2016. doi:10.1109/SP.2016.23.