Fully Decentralized Trading Games with Evolvable Characters using NFTs and IPFS

Christos Karapapas, Iakovos Pittaras, George C. Polyzos
Mobile Multimedia Laboratory, Department of Informatics
School of Information Sciences and Technology, Athens University of Economics and Business, Greece
{karapapas, pittaras, polyzos}@aueb.gr

***Abstract*—We leverage the InterPlanetary File System (IPFS) and Non-Fungible Tokens (NFTs) backed by Distributed Ledger Technologies (DLTs) to build a flexible, decentralized, and fair baseline system for trading games. Our solution creates a fully decentralized system, where new business models are enabled, as the evolvable assets of the games can be resold and priced depending on their rarity, giving also a cut to the digital artist, without the need for a trusted party. The system guarantees that assets will remain online, thus the users do not risk losing control over the artefacts or their value, even if the creator game company loses interest or goes bankrupt.**

***Index Terms*—Blockchain, DLT, Ethereum, Smart Contract, Authored Content, Digital Art, Non-Fungible Token**

I. Introduction

The growing popularity and maturity of DLTs has brought to the fore their use in gaming to address various problems faced by the industry. Offering unwavering proof of uniqueness and ownership, framed by currencies, is fertile ground for the development of various types of games, especially trading (card) games. In 2017, blockchain trading games made their appearance using tokens and since then they have been growing in popularity as well as in market capitalization. Despite their thriving, they bear a set of shortcomings. Non-Fungible Tokens (NFTs) are digital assets representing ownership of an extensive variety of unique, substantial, and potentially abstract but often concrete digital goods. The most popular are digital art and crypto-collectibles. At the time of writing, the all-time volume of the NFT market is around $436,527,057.[1]

As DLTs matured, the first DLT games began to appear, with some of them focused on crypto-collectibles. The first DLT-based game to flourish was CryptoKitties, released in 2017. Since then, many other cryptogames have appeared [1], like Sorare or Gods Unchained, a fantasy trading card game, among others. Although these games are characterized as Decentralized Applications (DApps), there is a pitfall that arises from the centralization of their media files. Artwork and metadata are important components of the asset and despite the fact that a user may own a NFT, typically she does not have ownership of the associated files as they are usually stored on the gaming company's servers.[2] Thus, questions arise: i) Who owns the artwork of the game? ii) Does the artwork have any value? iii) Anyone can have access to the artwork? iv) What happens to all the data if the company goes bankrupt?

[1]https://nonfungible.com/market/history

[2]https://medium.com/gmcmullen/do-you-really-own-your-cryptokitties-d2731d3491a9

ISBN 978-3-903176-39-3©2021 IFIP

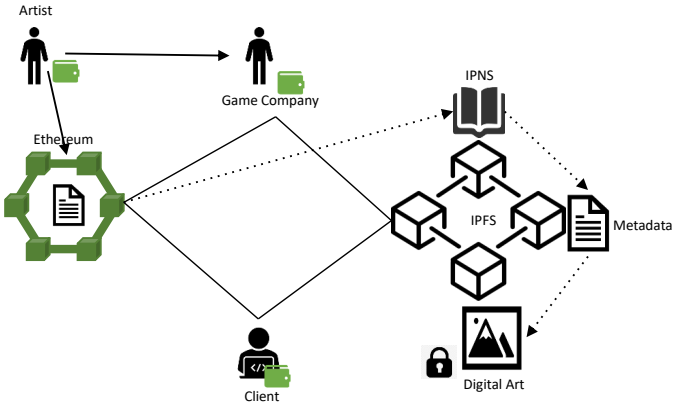

Fig. 1. Our reference architecture

It seems that decentralized file storage is imperative. IPFS is currently one of the best solutions, providing a P2P network for storing and exchanging data, with multi-platform software and a fast growing community. In addition, IPFS is complemented by IPNS, which is the naming system used by IPFS.

In our previous work [2], we investigated how DLTs can be combined with the IoT to create an open ecosystem for novel, dynamic, evolvable, context aware and fun games. In this paper, we go a step further, proposing using NFTs and Ethereum Smart Contracts (SCs) to build trading games which better retain asset value. We leverage IPFS and IPNS to reliably host Web pages serving as rendezvous points for SCs, as well as the metadata and the digital artwork files. Finally, we exploit threshold cryptography, where a secret is shared between n parties and a coalition of at least k of them is necessary to recover the secret, where $k < n$, for securely disengaging from the gaming company.

This design achieves the following: 1) The metadata and the artwork are stored on IPFS, which provides tamper-proof file storage. 2) Artwork gains value, as it is stored encrypted, and it is public whether the owner has decrypted and downloaded it. 3) It supports paying royalties to the artist (or other party) at every resale. 4) Enables evolvable characters that change avatars and attributes as they evolve over time. 5) All the data and assets will survive and stay online even if the gaming company becomes uninterested or bankrupt.

II. System Design

Our system considers the architecture depicted in Figure 1. There is an artist creating the digital art and a gaming company

2021 IFIP Networking Conference (IFIP Networking) | 978-3-9031-7639-3/21/$31.00 ©2021IFIPNETWORKING52078.2021.9472196

(game administrator/creator) that creates the smart contract that handles the tokens, deploys the smart contract on the (Ethereum) blockchain, encrypts, and stores the media (digital art) and metadata on IPFS adding the matching entries on IPNS. In order to perform these actions, the company needs to own an Ethereum wallet (corresponding to a public/private key pair). Furthermore, for each IPNS address needed, an extra pair of keys needs to be generated, as well as a symmetric key for each media file. In addition, there are clients, who interact with the (Ethereum) blockchain and IPFS in order to acquire (buy) a character (NFT) in the game; hence they also have to possess "accounts" on the Ethereum blockchain.

From a high-level perspective, the system works as follows. Initially, the game company implements the ERC-721 token standard in a smart contract and deploys it on the Ethereum blockchain. Then, it creates the tokens, receives the media files (e.g., character avatars) from their creator and initializes the corresponding IPNS entries. Subsequently, it generates a key to encrypt the media files. Upon encrypting them, it uploads them in IPFS and modifies the IPNS entries to point to the IPFS hash of the metadata. In the metadata file there is an entry with the hash of the media files on IPFS. As a next step, it modifies the tokens in the blockchain and for each token it changes the token URI field to point to the corresponding IPNS entry. Using Shamir's Secret Sharing $(2, 3)$ threshold scheme [3], it splits the key in 3 parts and each role of the system (artist, game company, client/buyer) acquires one. Finally, it creates a list for each token and stores it on IPFS (this list is also included in the metadata stored in the IPNS entry). This list contains the current owner of the token and a value that shows whether the media file has been downloaded and decrypted. The list is automatically updated by software owned by the game company, every time a token changes ownership, by "listening" to the blockchain for events.

When a client wants to acquire a character, she has to pay the defined amount of money (in ether) on the smart contract. Then, the tokens are "transferred" to her account (wallet), and she is able to see the metadata of the token stored on IPFS. If she wants to download and decrypt the digital art, she has to ask for the other parts of the decryption key through the smart contract. Then, the gaming company or the artist send their part of the key to the client offline and off-chain. The list showing that the client downloaded and decrypted the media files is updated. The price of the token is adjusted based on the status of the asset in this list, i.e. if an asset has not been decrypted by any user yet, its price remains high.

III. Discussion

In the blockchain-based token that represents the in-game character, in the metadata field, we store the IPNS entry and not the metadata of the character itself that can change arbitrarily, since we consider evolvable characters. By doing so, we ensure that when the character evolves, thus the digital art is updated, there is no need for a change in the smart contract, nor the token. Thus, we have lower gas consumption, which is typically non-negligible. Since, IPNS entries are stored in the DHT, if the game company goes bankrupt, the IPNS records will remain live for a short period of time although they are controlled by the game company.

Furthermore, by leveraging DLT and smart contracts in particular, our design allows providing royalties to the artists on every resale. More specifically, it provides the opportunity for the game company to be separate from the artist, e.g. outsource the artwork, and each time the asset is re-sold, the artist automatically receives royalties.

Moreover, we simulate the "mint in sealed box," a practice applied by collectors of tangible assets leveraging the following process: the artwork is uploaded on IPFS encrypted; if the owner of the token wants to decrypt it, she must ask for the key from the smart contract. Thus, the system assumes that the collectible came "out of the box" and this is recorded in the corresponding list. This strategy was adopted by Kings of Leon[3] but in a centralized form. This feature requires the existence of unencrypted low resolution digital art for in-game purposes and encrypted high resolution art otherwise. Only the token owner has access to the latter (and previous owners perhaps, if they decrypted it and kept copies).

With the current rules of IPFS, when a user requests content, then she becomes a provider for that content too, making it remain cached online as long as there is at least one provider. In addition, we can ensure that the content will be available for the long-term with the use of pinning services such as Pinata.

Finally, the use of IPFS combined with the threshold $(2, 3)$ cryptosystem ensures that even if the company decides to stop supporting the game or go bankrupt, then all the files will remain online and the owner will be able to recover and decrypt them. This is something that is not feasible in the current state of trading games. Furthermore, there are economic incentives that discourage parties to collude in order to decrypt the data offline. Thus, our system ensures the availability of all resources. Collectors will be able to continue controlling and exchanging, in addition to tokens, the artwork.

IV. Conclusion

We presented a class of token-based trading games using IPFS and Ethereum smart contracts. This approach has valuable properties and provides multiple benefits. The proposed approach can be extended in many ways. For example, a different business model can be considered that benefits from the Filecoin, in order to ensure persistent storage on IPFS. Future work is the development of such games or digital art trading markets and the theoretical and experimental evaluation of the security and economic properties.

Acknowledgment

Work supported by a grant from Protocol Labs Inc.

References

[1] T. Min, H. Wang, Y. Guo, and W. Cai, "Blockchain games: A survey," in *IEEE Conference on Games (CoG)*, 2019.

[2] I. Pittaras et al., "Beacons and blockchains in the mobile gaming ecosystem: A feasibility analysis," *Sensors*, vol. 21, no. 3, 2021.

[3] A. Shamir, "How to share a secret," *Commun. ACM*, Nov. 1979.

[3]https://www.rollingstone.com/pro/news/kings-of-leon-when-you-see-yourself-album-nft-crypto-1135192/