NFT Performance and Security Review

Anastasiya Lavrova[1,2] and Oleg Iakushkin[1,2(✉)]

[1] Lanit-Tercom Italia SRL, Bari, Italy
[2] Saint-Petersburg University, Saint Petersburg, Russia
o.yakushkin@spbu.ru

Abstract. In this article we review NFT token architecture and metadata storage options. We show the main disadvantages and risks of the existing NFT architecture and infrastructure. NFT minting performance was analysed on various distributed ledger technologies. The main problem of NFT technology that we highlight is its associated metadata storage options. Since in-secure Web2 based servers are allowed as a storage solution data that is associated with the NFT tokens can be corrupted, modified and lost. Thus harming the end user. We see the main solution for such issues in data blockchains proliferation as they would provide data immutability.

Keywords: NFT · Metadata storage · Architectural risks · Performance

1 Intro

NFT, a non-fungible token is a transferable digital asset. The key difference between an NFT and FT (fungible token), is its uniqueness, which makes it suitable for identifying a certain item. Thus, NFT encodes a unique digital artefact, while FT encodes a type of digital currency [1,3].

In other words, the feature of the NFT token is to create a single digital representation of some object. In turn, FTs are standard coins that are equivalent to each other.

From the point of view of smart contracts, NFT is encoded by a unique identifier [4]. The user accessing the smart contract is returned a link to the JSON file based on this identifier. The file can technically store any information and links to data that is not verifiable at the time of creation and release of the NFT token. At the moment, the most popular uses of NFT are representations in the format of tokens of objects of various spheres:

- digital art, music;
- virtual real estate;
- game assets;
- event tickets, attendance receipts;
- domain names [8];

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2022
O. Gervasi et al. (Eds.): ICCSA 2022 Workshops, LNCS 13377, pp. 217–228, 2022.
https://doi.org/10.1007/978-3-031-10536-4_15

– tokenized insurance policies and obligations [9].

Attempts are being made to link NFT to physical objects, for example, the NIKE CryptoKicks technology, patented in 2019 [7].

2 Life of an NFT

2.1 Artist Creates NFT - Minting

The artist calls the function, passing there two types of data:

– (Name, description, link to the picture, other metadata) - used to generate a JSON token file
– The royalties are a commission to the author for each resale of the token (depending on smart-contract it can be stored as in JSON, so in blockchain storage)

After payment of the commission to the platform the token is generated. The main properties of the token used in the process of its life:

– Holder - the smart contract based on which the token was created.
– Author - the creator of the token.
– Owner - the current owner of the token (is the only address that will change "during the life of the token").
– Metadata - link to appropriate JSON file.
– Royalties - percentage after each token resale.

2.2 Selling

By default, the sale function is not included in the token standards. Developers of decentralized applications that require the sale function are forced to independently implement the auction logic in their smart contract. Users who mint the NFT independently using third-party services, such as OpenSea, can use the provided functions of the platform, if such exist, or use AMM.

2.3 Automated Market Maker (AMM)

On traditional exchange platforms, buyers and sellers offer different prices for an asset. When users consider the specified price acceptable, they make a deal, and this price becomes the market price of the asset. Stocks, gold, real estate, and most other assets rely on this traditional market structure to trade. However, with the help of blockchain technology, the usual exchanges were decentralized and transformed into AMM. Instead of using the producer's and recipient's order book, AMMS relies on liquidity pools. For example, ETH-USDT is a pair where users can share their ETH and USDT liquidity to receive trading fees. The main feature of an automated market maker is how anyone can become a market maker due to the simplicity of the operation of adding funds to the pool. AMM is based

on a simple mathematical formula that takes different forms. The most common of them are $aTokenBalance(p) * bTokenBalance(p) = k$, where k characterizes a constant balance of assets that determines the price of tokens in the liquidity pool. For example, if AMM has ether (ETH) and bitcoin (BTC), every time ETH is bought, the price of ETH rises because there is less ETH in the pool than before the purchase. Conversely, the price of BTC decreases as there is more BTC in the pool. The pool remains in a constant balance, while the total value of ETH in the pool will always be equal to the total value of BTC in the pool. Only when new liquidity providers join them will the pool size increase. Visually, the token prices in the AMM pool follow the curve defined by this formula. dAMM is a scaled analog of AMM developed by StarkEx, see Fig. 1, with an off-chain operator processing transactions on L2, which is the only person trading under the AMM contract on L2 on L1. It simulates the logic of the contract and offers trading quotes based on the state of AMM at the beginning of the batch and subsequent L2 transactions included in the batch. At the end of the package, the Operator calculates all transactions by performing the net difference under the L2-based AMM contract. The operator must simulate the logic of the contract and apply it to the correct state of the accounts to ensure that the L1 contract can act as a counterparty to L2 transactions.

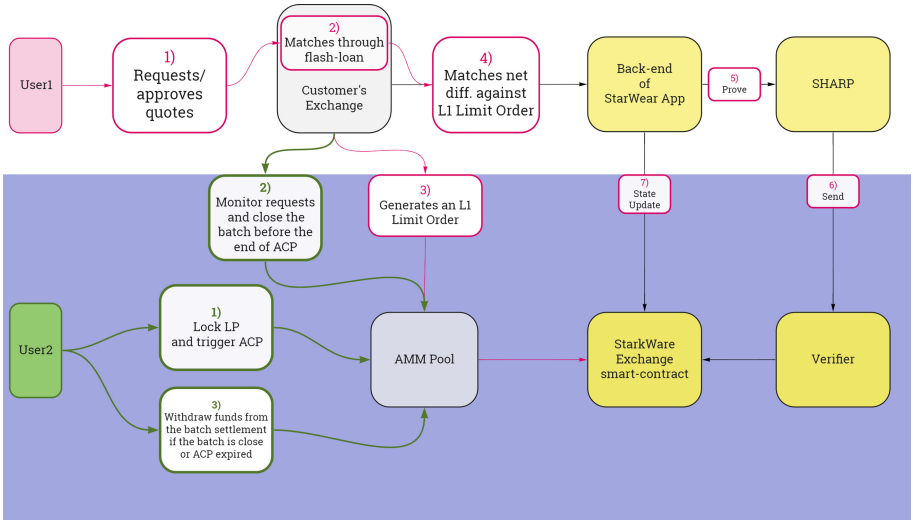

Fig. 1. AMM scheme for StarkEx ZK rollup. On blue background part that happens on Etherium main net, actions on taken by StarkEx apps. (Color figure online)

3 NFT Structure

Currently, many non-fungible tokens operate on the ERC-1155 and ERC721 Ethereum blockchain standards. In this article, we will mostly discuss the

Ethereum approach to NFTs. Yet most of the issues and solutions are similar across various blockchain networks. Thus recommendations of this article are broadly applicable. Services for demonstration, exchange, and creation of new NFT tokens are formed around the interfaces defined in these standards. The interface here implies a smart contract with a predefined minimum set of functions that are necessary for the correct operation of third-party applications, such as exchanges and crypto-wallets, see Fig. 2. The universal algorithm for creating an NFT looks like this:

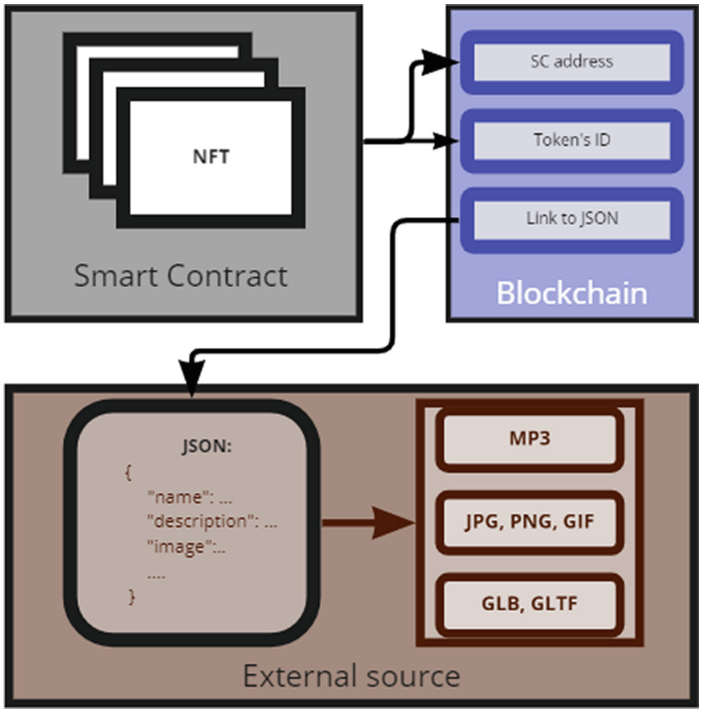

Fig. 2. Architecture of NFT token components' links

1. Creating a smart contract in which the project founder sets a set of basic characteristics for subsequent NFTs and configures additional functions to the basic template.
2. Minting is the process of creating a unique token.
3. Trading – token exchange between users.

Whenever an NFT is created or sold it is required to send a new transaction in the form of a request to the corresponding smart contract. After the transaction is confirmed, ownership information is added to the blockchain, thereby ensuring that the history of the NFT will remain unchanged and ownership will be preserved.

4 NFT Architecture Review

4.1 JSON Files

The problem of creating a universal NFT is to construct universal JSON files that will be supported by the main decentralized applications of any blockchain, see Fig. 3.

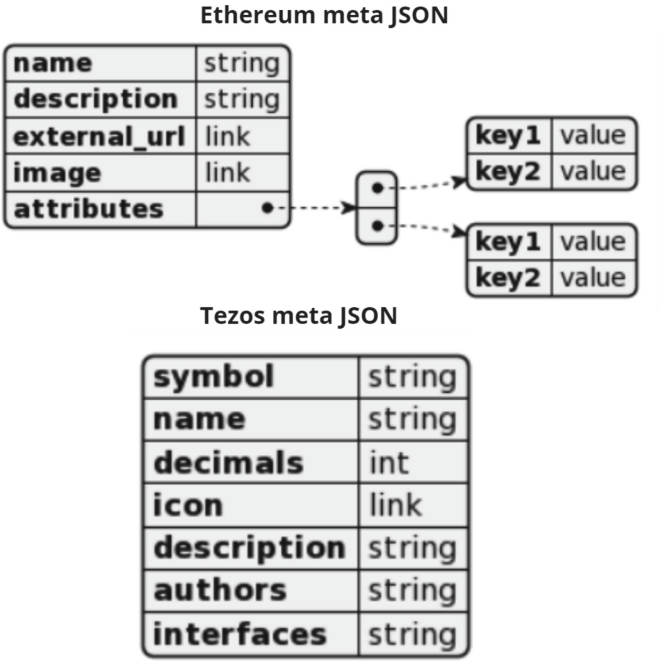

Fig. 3. Metadata format in different blockchains

4.2 Storage of Meta-Information and Media Data Options

The distributed registry itself contains the identifiers of unique tokens created by smart contracts and their owners. All characteristics of objects identified by tokens are stored as JSON files on third-party resources. In addition, each such JSON file contains links to media files that characterize the object "encoded" by tokens.

Currently, there are three different ways of storing characterizing information (JSON and media files) (Fig. 4):

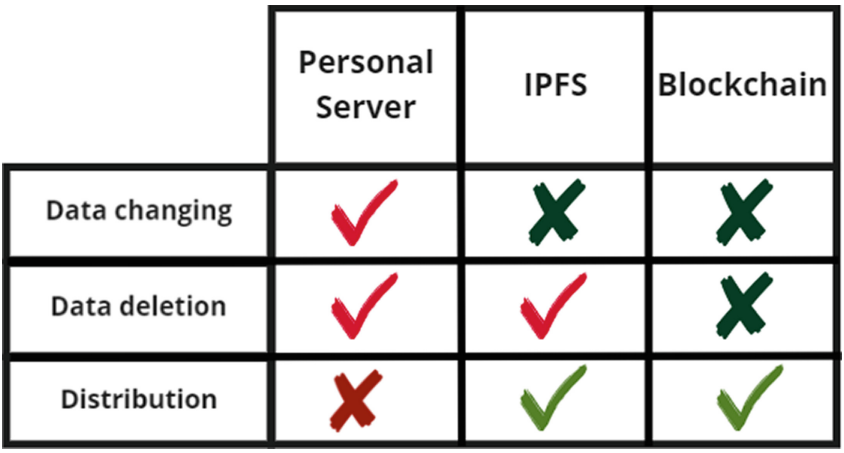

Fig. 4. Information storage methods (green - better, red - worse) (Color figure online)

1. Personal file server - the issuer of the NFT token can store files on its HTTP server. This option is the least secure way, due to the possibility of changing or deleting the relevant files by any user with access to the server.
2. IPFS (Interplanetary File System) is a decentralized data storage network. A unit of data transmitted in such a network is a block that can contain both parts of a file and links to other blocks. The file itself (or a directory of several files) is assembled from an oriented acyclic graph (DAG), which is based on certain blocks. IPFS provides the user with unique links containing a hash of data, making it much more difficult to replace them. The NFT containing links to meta and media data in IPFS cannot be changed, however, if there are no nodes left storing block data, the user will also receive an error when trying to view the contents of his NFT. The NFT issuer can manage its own IPS node, ensuring the availability of exactly those files that are associated with the NFT tokens issued by it. At the same time, the user is guaranteed that the content of meta and media files will not change.
3. File storage blockchain is a decentralized network that stores fragments from several old files when each new file appears. This approach is more reliable than IPFS, thanks to the consensus algorithms [5] and the replication of data from the past: data stored in a distributed registry cannot be deleted or replaced. However, storing large files in such systems can be very expensive. Currently, blockchains optimized for storing large files, such as Arweave, are emerging, but they are just beginning to gain popularity and are supported by fewer crypto wallets. If the number of users of these newly emerging blockchains for storing files is greatly reduced, data loss is inevitable, which the NFT issuer will not be able to control.

It is important to note that links to metadata and media files are carried out over HTTPS, which means that the files receive a domain name as part of the links. This means that when the domain is blocked, access to metadata is no longer available.

4.3 Options for Interacting with NFT Content

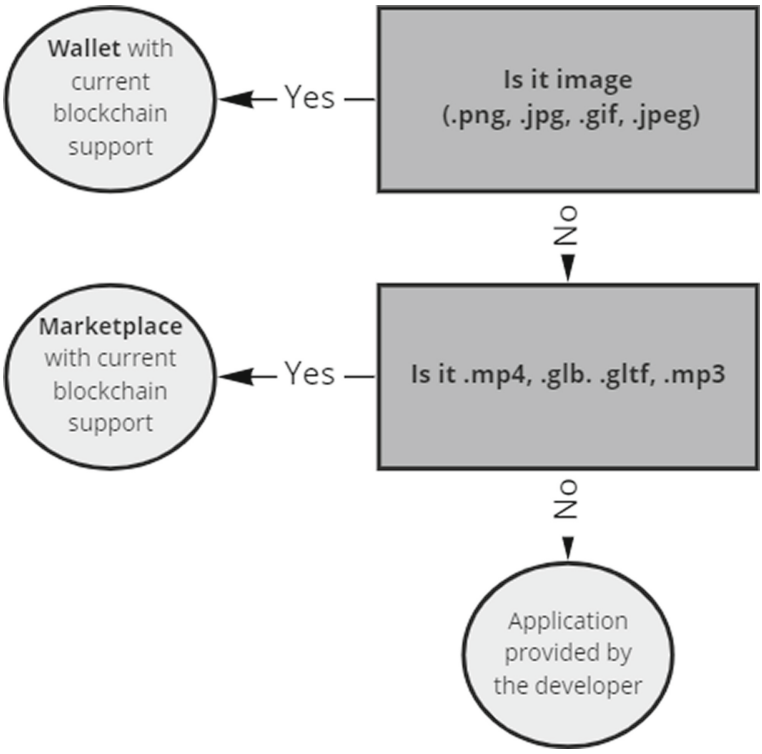

Fig. 5. Information storage methods

As it was shown on Fig. 5, the main components of NFT are records in the blockchain, meta-information, and media data, i.e., the ownership of NFT is fixed in the blockchain, but in a form unsuitable for viewing by the user. Therefore, despite the variety of metadata storage options, the unique token number will be displayed the same in all NFT-compatible crypto wallets of the user. However, it is worth noting that the methods of managing and viewing the token will be different in each case.

NFT digital creativity, such as visual files, music files, and 3D files, the user can view and manage using NFT-compatible crypto wallets supporting the corresponding blockchain or on specialized NFT markets. However, for example, Metamask will allow the user to view only two-dimensional images, while OpenSea will correctly display three-dimensional and audio files in addition to images. Thus, differences in presentation systems and the lack of consistent, open storage rules lead to inadequate support for data stored in NFT.

5 Ethereum Scaling

The number of transactions of the Ethereum network per day exceeds 1 million [10]. However, due to this popularity, the demand for limited computing resources of the network is increasing. The increase in the cost of gas causes significant transaction costs for users. In order to increase the performance of the Ethereum network without compromising security and decentralization, it was decided to scale Ethereum.

Ethereum scaling solutions are divided into on-chain and off-chain scaling.

5.1 On-Chain Scaling

This option implies modification of the main Ethereum network. Scaling is achieved using Sharding technology. It divides transactions into segments, allowing each node of the network to process not the entire block, but only its components.

5.2 Off-Chain Scaling

This option implies the development of a separate solution from the Mainnet. Security in such systems is provided either directly from the Ethereum Mainnet consensus algorithms (Optimistic Rollups, zkRollups), or independently (sidechains, plasma).

Optimistic Rollups. The main idea of the solution is that by default transactions on L2 are considered legitimate. Calculations will be made only in case of suspected fraud.

Zero Knowledge Rollups. Such a solution combines off-chain transactions and generates a specialized cryptographic proof with zero-disclosure SNARK. It allows the proving party to confirm the truth of the possession of information, without the need to disclose it.

Plasma. This solution is a separate blockchain tied to the main network. It allows you to create chains within the main networks, thereby ensuring scalability. The main Ethereum network is connected to the subsidiary "root contracts", which are Ethereum smart contracts, which contain the basic rules for managing each subsidiary chain.

Side-Chains. This solution is an independent blockchain. It is functionally compatible with the Mainnet Ethereum, that is, it allows assets to move between networks. As soon as the assets are in another blockchain, they are frozen in the original one.

6 Main Technological Issues We See in NFT Technology

We have tested several networks providing NFT minting capabilities and have detected the following disadvantages:

1. slow processing of operations,
2. high gas cost,
3. blockchain compatibility,
4. unavailability of NFT data.

6.1 Slow Processing of Operations

Since operations related to NFT are processed by sending transactions through smart contracts and are validated through a single blockchain network for all users, the confirmation time of operations is extremely slow. This problem is solved by scaling the Ethereum network using extensions (for example, L2 and Rollups). Such a solution will greatly increase the complexity of application development and the difficulty of logging in for users.

For comparison, we conducted an analysis in the official testnets of the Ethereum and Tezos blockchain, as well as on scalable Ethereum using ZKSync.

The speed of NFT generation on various blockchain test networks can be found on Fig. 6.

It can be noted that the time for generating tokens in the scaled Ethereum network significantly exceeds the time in conventional test networks. This is because initially the token is generated on L2, however, to perform operations on it, it is necessary to wait for generation, which takes a considerable time. Similarly with the output to L1 - despite the fast speed of operation, confirmation of the operation takes a long time. Speed of creating and displaying NFT in ZkSync testnet for 1 token can be found in Appendix C.

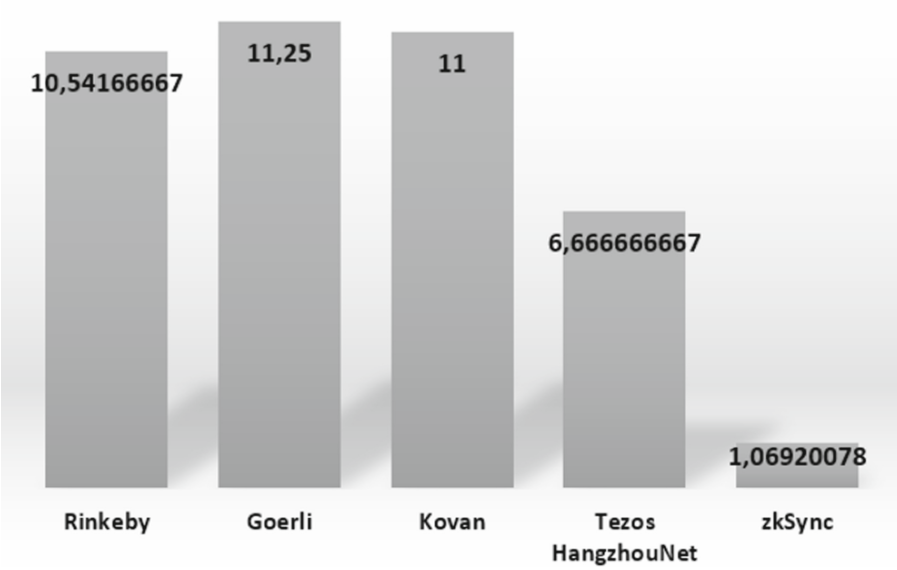

Fig. 6. Proportional minting time difference between 10 and 100 NFT tokens on different blockchain platforms (Testnets)

6.2 High Gas Cost

Each NFT-related transaction is more expensive than a simple transfer transaction because smart contracts require computing resources and storage to process. To avoid paying gas, you can use alternative platforms for creating tokens, such as Open Sea, or by switching to a less popular blockchain, such as BNB Smart Chain, Polygon, Solana, and others. We compared some of them, on Fig. 7.

6.3 Blockchain Compatibility

Existing blockchain systems are isolated from each other, i.e. by purchasing a picture on the Ethereum network and deciding to reduce the gas fee, it will be hard to transfer your picture to another blockchain. The inability to transfer your gaming equipment between two identical games based on different blockchains is also a significant obstacle to the introduction of the NFT ecosystem into crypto games [6]. However, many NFT-related projects use Ethereum as the base platform due to its liquidity capacity. Another solution that is gaining popularity is cross-chain bridges that transfer user assets between wallets of different blockchains shown on Fig. 8.

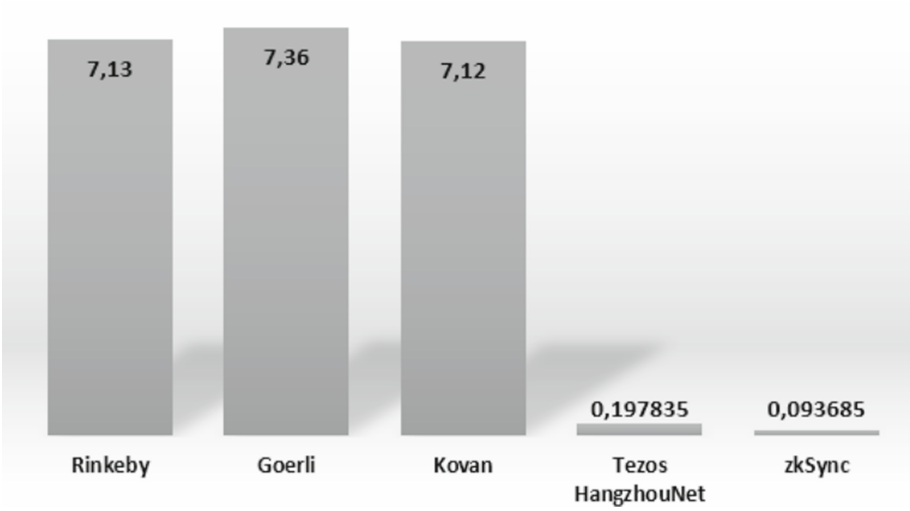

Fig. 7. Price of minting on testnets in USD

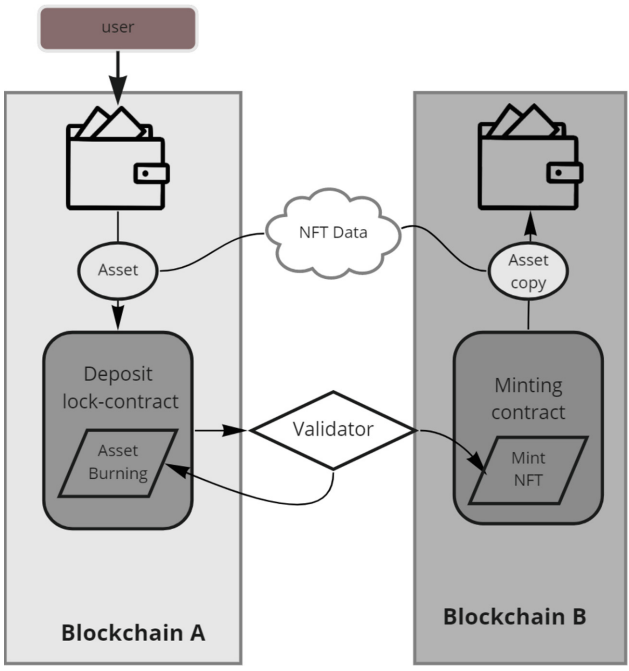

Fig. 8. Cross-chain bridge scheme.

6.4 Unavailability of NFT Data

Due to data storage outside the main blockchain, data may disappear or change. An error can be made during the creation of meta-information for a token by specifying the addresses of the corresponding metafiles. In this case, the user will own only a record in the blockchain without the ability to view their assets.

7 Conclusion

The article discusses the NFT token architecture, metadata storage options and highlights the main disadvantages of the existing NFT architecture and infrastructure. The issues of storing multi-media data of NFT tokens are analyzed. The most acute problem, according to the authors, is the possibility of a loss of access or substitution of user files. Such a danger arises due to the possibility of media files stored outside of the distributed registries. Also, it shall be noted that there is a persistent lack of requirements, rules, and guidelines to ensure the security and uniformity of metadata stored in the main standards describing NFT (ERC-721 and ERC-1155).

References

1. Chohan, U.W.: Non-Fungible Tokens: Blockchains, Scarcity, and Value. Critical Blockchain Research Initiative, Sidney (2021)
2. Shurov, A., Malevanniy, D., Iakushkin, O., Korkhov, V.: Blockchain network threats: the case of PoW and ethereum. In: International Conference on Computational Science and Its Applications 2019, Sydney, pp. 606–617 (2019)
3. Mieszko, M.: Non-Fungible Tokens (NFT). The Analysis of Risk and Return. ESSCA school of management, Paris (2021)
4. Akash, A., Shailender, K.: Smart contracts and NFTs: non-fungible tokens as a core component of blockchain to be used as collectibles. In: Khanna, K., Estrela, V.V., Rodrigues, J.J.P.C. (eds.) Cyber Security and Digital Forensics. LNDECT, vol. 73, pp. 401–422. Springer, Singapore (2021). https://doi.org/10.1007/978-981-16-3961-6_34
5. Rehmani, M.H.: Blockchain consensus algorithms. In: Blockchain Systems and Communication Networks: From Concepts to Implementation. TTE, pp. 61–78. Springer, Cham (2021). https://doi.org/10.1007/978-3-030-71788-9_4
6. Chen, J.-T.: Blockchain and the feature of game development. In: Hung, J.C., Yen, N.Y., Chang, J.-W. (eds.) FC 2019. LNEE, vol. 551, pp. 1797–1802. Springer, Singapore (2020). https://doi.org/10.1007/978-981-15-3250-4_239
7. Patent NIKE CryptoKickss. https://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&p=1&u=/netahtml/PTO/search-bool.html&r=1&f=G&l=50&co1=AND&d=PTXT&s1=Nike&s2=Crypto&OS=Nike+AND+Crypto&RS=Nike+AND+Crypto. Accessed 26 Apr 2022
8. Unstoppable domains. https://unstoppabledomains.com/. Accessed 26 Apr 2022
9. Yinsure.finance. https://yinsure.finance/. Accessed 26 Apr 2022
10. Ethereum Daily Transactions Chart. https://etherscan.io/chart/tx. Accessed 26 Apr 2022