Trading Security Designs Based on Blockchain Techniques

Chang Liu*

Dublin College, Peking University of Technology, Beijing, China

*Corresponding author: chang.liu5@ucdconnect.ie

Abstract. Contemporarily, digital art has swiftly integrated into human beings' daily life. While digital art is becoming increasingly popular and significantly influences conventional art, currently it is needed to be more online communities where art enthusiasts and artists may interact and offer a self-sustaining means of payment. Independent art programs based on ideas like reciprocity are what E-Gallery Art aspires to. Its goal is to encourage teamwork and co-creation in the visual arts. This research discusses the way to create decentralized Dapps based on blockchain that are mutually advantageous for platforms, artists, and users. The Dapp follows a process where users reward artists by donating, and the best-case scenario is that the artist is motivated and contributes more to the community. Users can create galleries and display their work for free, which is an important starting point for E-Gallery Art Dapp to start a self-sustainable cycle. These results shed light on guiding further exploration of trading security design based on blockchain techniques.

Keywords: Trading security; Blockchain; Dapps.

1. Introduction

With the wide application of various digital painting technology and artificial intelligence painting technology, the number of painting works based on electronic data increases rapidly [1-3]. The usage of digital painting can bring more convenience and more significant economic benefits to the creator group. Many new digital painting trading institutions have appeared recently to ensure the average circulation and use of digital images. In addition to traditional data circulation methods, a big data trading market facilitates data trading by matching data requirements with data sources.

In a common data market, the data are provided by the data seller to a centralized trading platform, which then stores the data. Even though the data trading platform makes the flow of data more efficient, there is still plenty of problems [4]. Once the malicious party has gotten the data, it is possible for them to resell the seller's data by caching the source data at a price that is lower than what the seller charges, which is detrimental to the seller's interests. Once an attacker has gained access to a centralized trading platform, it may be paralyzed if the platform has low fault tolerance. This would affect the data transaction between the data buyer and the data seller and may even result in the loss of essential data. The technology known as blockchain is a recent advancement in the field of secure computing that does not rely on centralized authority and operates inside an open networked environment.

The participants of a blockchain system trust the legitimacy of all transactions recorded on the chain, and the chain's growth makes it computationally impossible to alter any one block without being noticed. These two factors contribute to the blockchain system's reputation as a safe and secure platform (cryptographic hashes iteratively link, i.e., blocks) [5]. A blockchain is like a distributed database that tracks an ever-expanding list of transaction records by arranging them into a hierarchical chain of blocks. This kind of database is useful for managing data in a decentralized manner. Regarding safety, the blockchain is built and controlled via a peer-to-peer overlay network and protected by intelligence. It is guarded by sophisticated, decentralized use of encryption and computer power provided by a crowd [6].

The first few stages of blockchain development have potential advantages for businesses, including security, automatic record keeping, immutability, and the potential to pay invoices, bills, and wages within a secure framework. However, there is still room for speed and ease of use improvement. Blockchain 4.0 aims to enhance the user experience in the industry. It is built on decentralized,

trustworthy, and encrypted ledgers and allows businesses to shift part or all of their present activities onto secure, self-recording apps. This feature of the system was created specifically for businesses.

The remaining parts of this work are organized as described below. The second section of this article covers the fundamentals of describing blockchains and trading systems. In Section 3, this study will discuss the security designs that are based on blockchain technology. Section 4 will demonstrate how our security architecture works in practice. Contemporaily, Section 6 will wrap up the discussion by analyzing the shortcomings of our demonstration.

2. Basic Descriptions of Blockchain and Trading System

The core concept of blockchain is to build related data blocks that can be verified by each other (i.e., blocks), sort the blocks by time stamps, and combine cryptography technology to form a network value transmission system with collective maintenance, mutual verification, and orderly links. There are a few core concepts one needs to understand about blockchain. A block is a carrier used to store data information. Valuable information is kept forever as data in blockchain technology. Each block contains information on the transactions that occurred at the time it was produced and is sorted in chronological order. All blocks are interconnected to create a "global ledger," with each block serving as a page. A tyical sketch of the blocks function in blockchain is shown in Fig. 1.

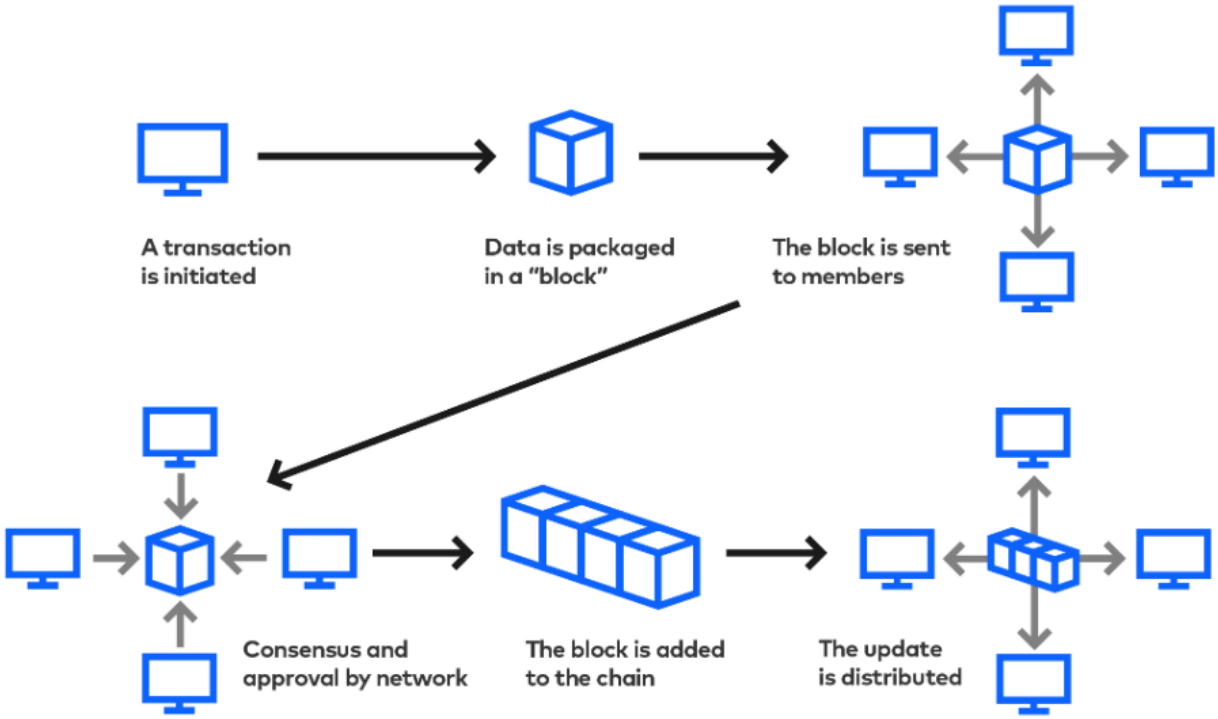

Fig. 1 A Sketch of transaction for blockchain.

Ethereum has been the most widely used blockchain platform for smart contracts since its launch in July 2015. With the help of a global network of public compute nodes, Ethereum offers a decentralized Turing-complete machine called the Ethereum Virtual Machine (EVM) for script execution. Programming languages like Solidity11 and Vyper12 may be used to create sophisticated smart contract applications on Ethereum. All smart contracts made using high-level programming languages would be translated into Ethereum bytecode and run by the EVM. Additionally, Ethereum has its cryptocurrency called Ether. Ether may be used to pay participants whom mine blocks for calculations done and be transferred between accounts [7, 8]. A sketch of the Ethash hashing algorithm for Ethereum is presented in Fig. 2

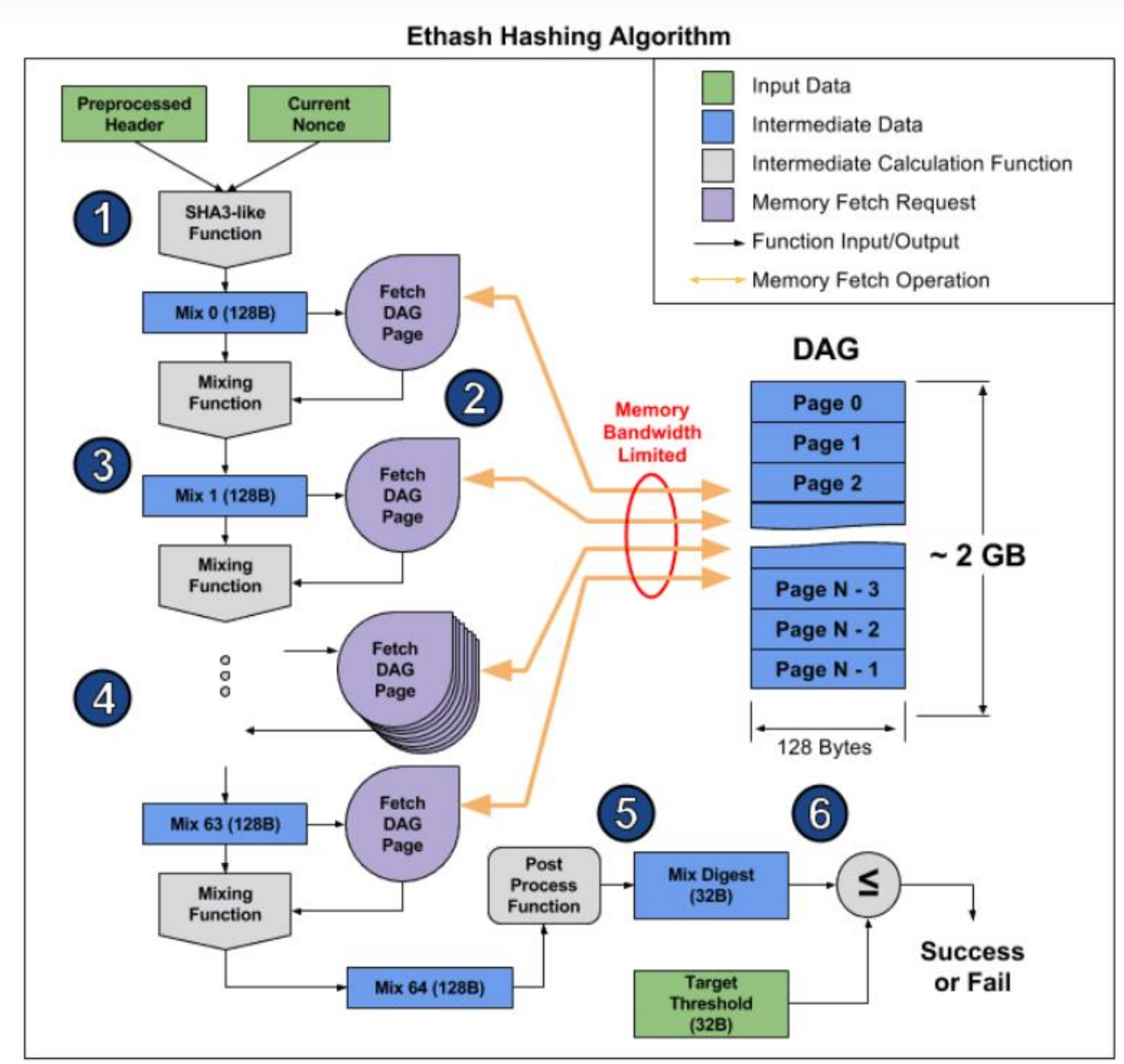

Fig. 2 A Sketch of Ethash hashing algorithm for Ethereum.

The smart contract is a piece of software recorded on the blockchain and may run automatically when specific criteria are satisfied. Once the requirements are satisfied, the contract will automatically and forcibly execute to change the blockchain's states or values without any restrictions. Consequently, trust between two parties can build without using a reliable third party. The smart contract is a piece of software recorded on the blockchain and may run automatically when specific criteria are satisfied [7]. Once the requirements are satisfied, the contract will automatically and forcibly execute to change the blockchain's states or values without any restrictions. Consequently, trust between two parties can build without using a reliable third party.

NFTs are unique certificates of authenticity that are frequently provided by the people who produced the underlying assets on blockchains. These resources might be physical or digital commodities that can be exchanged for other items of the same kind, such as money or tradeable items. Non-fungible goods, on the other hand, cannot be exchanged for a similar good since their value exceeds that of the raw materials.Non-fungible items have proven difficult to trade and auction in the digital age due to the impossibility of validating their existence. NFTs enable the digitization and trading of unique assets via the internet [9].

Blockchain technology is the integration of cryptography, economics, distributed storage technology, network science and application data, and other technologies, aiming to build a set of trusted value transmission systems. These technologies are combined according to specific rules to create a set of distributed data recording and storage systems. The time stamps are used to sort the blocks of stored data, forming a continuous and related distributed database, which is the natural carrier of value.

3. Security Designs

This study tried to find and build an efficient design for the E-gallery Dapp. Because NFT is a one-of-a-kind token that cannot be swapped for another of the same kind, often known as being non-fungible, it is well suited for uniquely identifying something or someone. To be more specific, a creator may demonstrate the existence of digital assets like as films, photographs, works of art, event tickets, and so on by using non-fungible tokens (NFTs) on smart contracts. It is well secured that the selling values of these IP-related items, which may have looked unimaginable for non-fungible virtual assets; instead, are properly protected [10], where a workflow of NFT system is presented in Fig. 3.

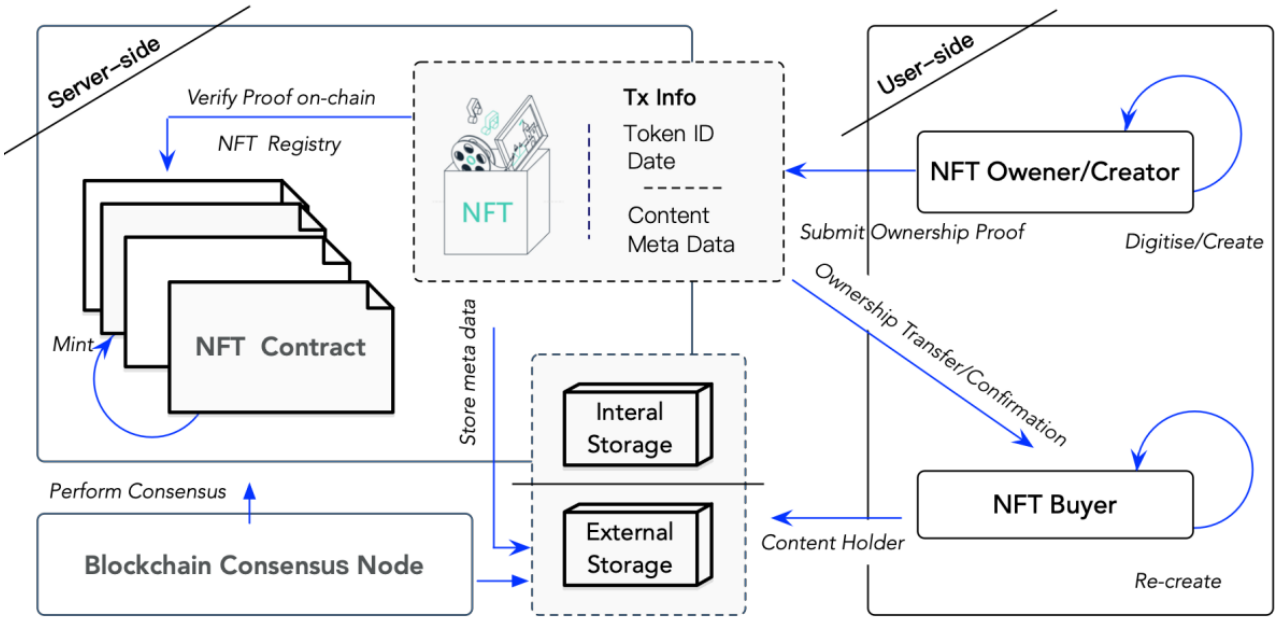

Fig. 3 A workflow of NFT.

In this Dapp, the resolution of digital painting combined with an NFT token can ensure the individual copyright for the image. Meanwhile, the usage of the marketplace paid by artists and transactions of the NFT token can provide fees to access the blockchain or produce benefits. Therefore, the NFT token can solve the problems of copyright security and gas fee payment. Many NFT web platforms, such as OpenSea [11], introduced the IPFS as the solution to save metadata and images in a decentralized system. Therefore, one decided to achieve the E-gallery prototypes using a gateway API to upload or get information from the IPFS. The IPFS gateway, such as the Pinata or Infura, can provide a convenient and efficient solution for IPFS interaction and may decrease the cost of using the IPFS. The NFT token and purchase contracts are deployed on the Georli test network. Users can interact with the front-end components implemented by the web3 dependency to access the IPFS or deployed intelligent contacts. In addition, the payment and identifying services will be provided by Metamask. For development, one used the React-Truffle architecture to build the DApp.

NFTs, or non-fungible tokens, are unique certificates of authenticity that may be used on blockchains. The same people who produced the underlying assets often provide these certificates. These resources are either physical or digital in nature. It is possible to exchange fungible things, such

as money or trade products, for other objects of the same kind. On the other hand, non-fungible commodities cannot be traded for anything equivalent since their value exceeds the value of the raw materials they are made from. This prevents them from being traded. Rare trading cards, antiques with historical or aesthetic value, and other commodities that have a long history of being sold at auctions and different marketplaces are some examples of things that may be found in the analog world. Because it is hard to verify the veracity of non-fungible things, trading and auctioning these types of items in the digital world has proven difficult. The digitization and trading of one-of-a-kind assets are now made possible via NFTs. A sketch to ensure the trading security is presented in Fig. 4.

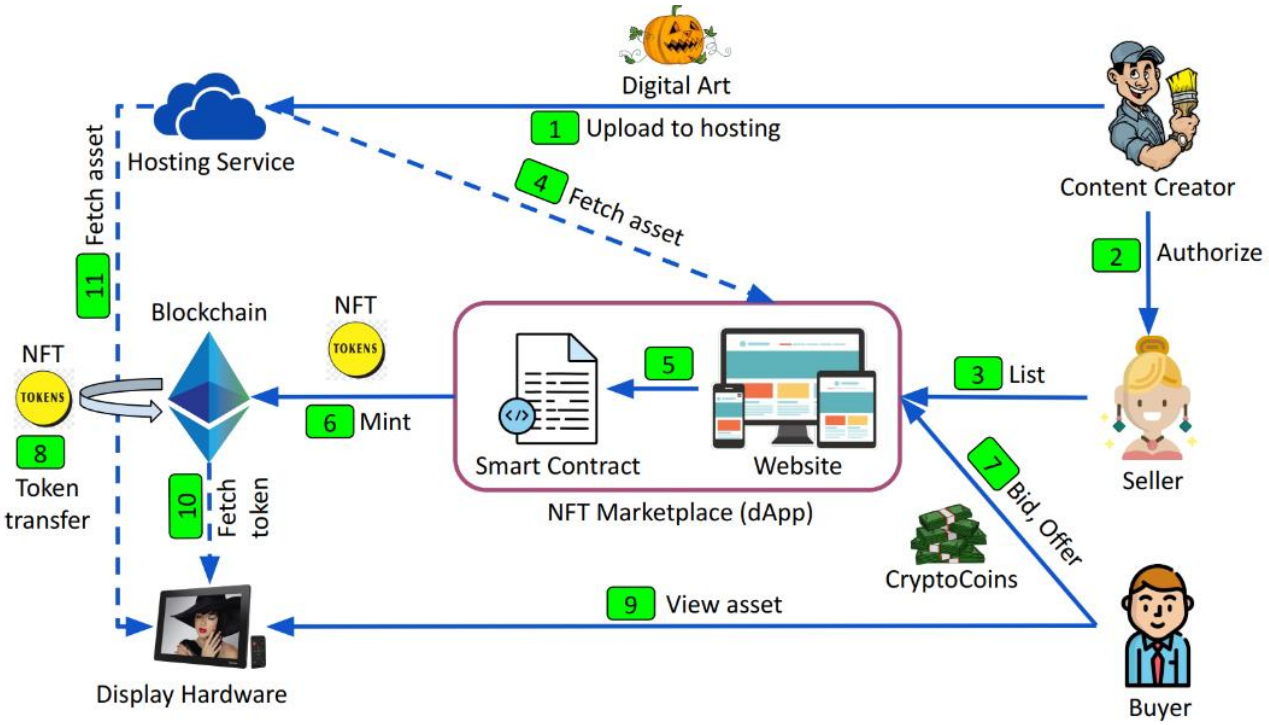

Fig. 4 A Sketch of trading secruity designs of NFT.

4. Demo

This study started the development process by putting together dApp and configuring the environment. As the front-end framework, React will be used for this study, and the back-end framework will be utilizing the Truffle box. One primarily implemented four functions in the front-end react.js application. These were browsing the photos items, examining the details of the images items, buying to get the NFT token for images, and publishing new images item functions.

To facilitate user identification, login, activating the wallet to transmit the transactions, and more, one uses MetaMask, a free, open-source wallet for the Ethereum digital currency that facilitates secure and convenient storage and management of all associated digital assets. To publish new images item function, once one user publishes an image item, the original images will be sent to the blockchain and stored as one block by IPFS of infura. Meanwhile, the blurred images from this item will be held in a database along with other information about the image, such as the author's name and work details, so those potential buyers can learn more about the work when they browse the unit. As for purchasing function, once one user buys an image item, he pays for gas in exchange for an NFT token, which contains the block address of the original image on the blockchain, through a smart contract provided under the Truffle framework.

5. Limitations & Prospects

In the next step, one nees to improve our Dapp mainly from two areas: Increments and iterations. In iterations, researchers will enhance our platform's security: improve the MongoDB connection and the simplified function in case hackers can't get the original picture directly from the web page, and ensure that only after a buyer receives the token can he get the original painting. In increments, one will improve the web's UI and update the layouts of the pages. Moreover, it is necessary to add the tag mechanism on paintings to improve the search function, add donation incentives and a popularity recommendation mechanism.

6. Conclusion

In summary, this paper investigates the trading security designs of Dapp based on blockchain techniques. According to the analysis, it is clear that even though platforms provide mature methods for selling and trading artworks, there still needs to be more solutions for enhancing cooperation between users, artists and the platform. The Dapps can therefore use a unique self-sustainable procedure to strengthen relationships between users and the platform to contribute to the community. One also needs to provide clear instructions to users and suggest they support the artist they like. Overall, these results offer a guideline for security designs of trading in terms of blockchain approaches.

References

[1] Zhong M. Study of digital painting media art based on wireless network. Wireless Communications and Mobile Computing, 2021, 2021.

[2] Luo W, Yang J, Hua Y. Research on the aesthetic mode of digital painting based on digital technology. 2016 International Conference on Smart Grid and Electrical Automation (ICSGEA). IEEE, 2016: 304-307.

[3] Yin S. Analysis on the Inner Relationship between Computer Digital Painting and Traditional Painting. Mobile Information Systems, 2022, 2022.

[4] Liu H, Tai W P, Wang Y, et al. A blockchain-based spatial data trading framework. EURASIP Journal on Wireless Communications and Networking, 2022, 2022(1): 1-17.

[5] Zhu L, Wu Y, Gai K, et al. Controllable and trustworthy blockchain-based cloud data management. Future Generation Computer Systems, 2019, 91: 527-535.

[6] Zhang R, Xue R, Liu L. Security and privacy on blockchain. ACM Computing Surveys (CSUR), 2019, 52(3): 1-34.

[7] Zou W, Lo D, Kochhar P S, et al. Smart contract development: Challenges and opportunities. IEEE Transactions on Software Engineering, 2019, 47(10): 2084-2106.

[8] Chen T, Li X, Luo X, et al. Under-optimized smart contracts devour your money. 2017 IEEE 24th international conference on software analysis, evolution and reengineering (SANER). IEEE, 2017: 442-446.

[9] Ante L. The non-fungible token (NFT) market and its relationship with Bitcoin and Ethereum. Available at SSRN 3861106, 2021.

[10] Wang Q, Li R, Wang Q, et al. Non-fungible token (NFT): Overview, evaluation, opportunities and challenges. arXiv preprint arXiv:2105.07447, 2021.

[11] White B, Mahanti A, Passi K. Characterizing the OpenSea NFT marketplace. Companion Proceedings of the Web Conference 2022. 2022: 488-496.