DOI: https://doi.org/10.53052/9788367652001.09

Vasyl POBEREZHNYK[1], Oleh HARASYMCHUK[2], Ivan OPIRSKYY[3]

Supervisor: Ivan OPIRSKYY

OCHRONA PLIKÓW MULTIMEDIALNYCH PRZED FAŁSZOWANIEM I NIELEGALNYM WYKORZYSTANIEM W OPARCIU O BLOCKCHAIN

Streszczenie: Ten artykuł poświęcony jest podstawowym zasadom działania blockchain, tworzeniu podpisów NFT dla obrazów i tworzeniu bezpiecznej metody generowania tokenów NFT, aby zapobiec kradzieży oryginalnych plików przez skompromitowaną platformę rynku NFT, zapewniając mechanizm bezpiecznego generowania tokenów po stronie twórców bez zaangażowanie strony trzeciej. Podano również zalecenia dotyczące ochrony e-portfela.

Słowa kluczowe: blockchain, Ethereum, NFT, smart kontrakt, kryptografia, e-portfel, transakcja cyfrowa, haszowanie, kryptowaluta

MEDIA FILES PROTECTION AGAINST FORGERY AND ILLEGAL USE BASED ON BLOCKCHAIN

Summary: This article dedicated to the basic principles of blockchain operation, the creation of NFT signatures for images and creation of secure method for NFT token generation to prevent original file theft through compromised NFTs marketplace platform by providing mechanism to secure token generation on the creators' side without involvement of third party. Also, the recommendations for e-wallet protection were given.

Keywords: blockchain, Ethereum, NFT, smart contract, cryptography, e-wallet, digital transaction, hashing, cryptocurrency

1. Introduction

Recently, Blockchain technology is increasingly taking over the entire market. With the emergence of P2P payment systems such as Bitcoin and Ethereum, the number of people interested in buying and selling digital coins is increasing. There are also other uses for Blockchain: secure transfer of medical data, border transfers, voting

[1] Lviv Polytechnic National University, postgraduate student of Information Protection Department, vasyl.o.poberezhnyk@lpnu.ua

[2] PhD, Lviv Polytechnic National University, Associated Professor of Information Protection Department, oleh.harasymchuk@gmail.com

[3] DSc, Lviv Polytechnic National University, Professor of Information Protection Department, iopirsky@gmail.com

mechanism in elections, tracking of music royalties, real estate processing platforms, etc.

Another option is the NFT market. In 2014, the first NFT (nonfungible token) appeared from Kevin McCoy and Anil Dash. This is the first time that a non-replaceable Blockchain token has appeared on a Blockchain chain [1].

In 2019, Nike patented a system called CryptoKicks that uses NFTs to verify the health of the sneakers and give the customer access to a virtual version [2]. Now users choose NFT for selling your own creations.

Counterfeiting is a problem with NFT artwork. It's easy to make collectors wonder if some digital art they have paid for is really a genuine Banksy piece or just a fake. To solve this problem, some platforms use an old-fashioned method of verifying creators' identity on their platform: manual verification. For example, SuperRare requires artists who wish to publish their digital works for sale on its platform to apply form, which requires information such as name, email, artwork selection, social media presence, and more. These allows SuperRare to ensure that collectors receive authentic artwork by reputable artists who hold the appropriate rights to the underlying art.

Other NFT markets try to avoid counterfeiting problems by using broad limits. For example, if a user tries to buy something through the AtomicAssets marketplace, it is compressed with the following message, which the user must accept in order to move forward with the purchase: "Anyone can create NFT AtomicAssets and choose attributes such as name and image, including fake versions. existing NFTs or stolen intellectual property. Before buying an NFT, always do your own collection research and check the collection name to make sure you are buying a real NFT" [3].

For example, on December 2, 2021, an NFT by Pak called "The merge" was sold for $91.8 million. Another example is the sale of Beeples work called "Everydays: The First 5000 Days" for $69 million. Moreover, analysts predict the growth of the NFT market to 231 billion dollars by 2030[4], which makes it a promising market, on the other hand, a mixed one for attackers, who can become victims not only of platforms selling NFTs, but also of the creators themselves.

The purpose of this work is to create a concept of protection of media files against forging and illegal use based on blockchain technology.

2. Blockchain and NFT basics

2.1. Blockchain

A blockchain is a list of records, called blocks, connected to each other using cryptography. Each block contains the cryptographic hash of the previous block, a timestamp, and transaction data. The timestamp proves that the transaction data existed at the time the block was published in order to get into its hash. Blocks contain the hash of the previous block, forming a chain, each additional block is added before it. This means that if one block in one chain were altered, it would be immediately obvious that it had been tampered with. If hackers wanted to corrupt the blockchain system, they would have to change every block in the chain in all distributed versions of the network what is impossible. Blockchains like Bitcoin and Ethereum are constantly growing as blocks are added to the chain, greatly increasing security.

Most common databases, such as SQL databases, have an administrator who can modify records. Blockchain is different in that there is no administrator; it is run by the people who use it. A decentralized blockchain can use dedicated messaging and a distributed network. One risk of a lack of decentralization is a so-called “51% attack,” where a central authority can gain control of more than half of the network and can manipulate that blockchain record at will.

In blockchain networks, there is no centralized point of vulnerability that can be exploited by computer hackers; nor does it have a central point of failure. Blockchain security techniques include the use of public key cryptography. Each node in the decentralized system has a blockchain copy. Data quality is supported by massive database replication and computational trust. No centralized "official" copy exists, and no user is "trusted" more than any other. Transactions are broadcast to the network using the software. Mining nodes verify transactions, add them to the block being built, and then transmit the completed block to other nodes.

To carry out a transaction, node needs to solve the incredibly difficult mathematical task of finding the nonce that generates the accepted hash. This task is solved by miners - computers in the network that receive a commission for conducting a transaction. Since a nonce is 32 bits and a hash is 256, there are approximately four billion possible nonce-hash combinations that must be extracted before the correct one is found. When this happens, miners say they have found a "golden nonce" and their block is added to the chain. Thus, any transaction is performed (Fig. 1).

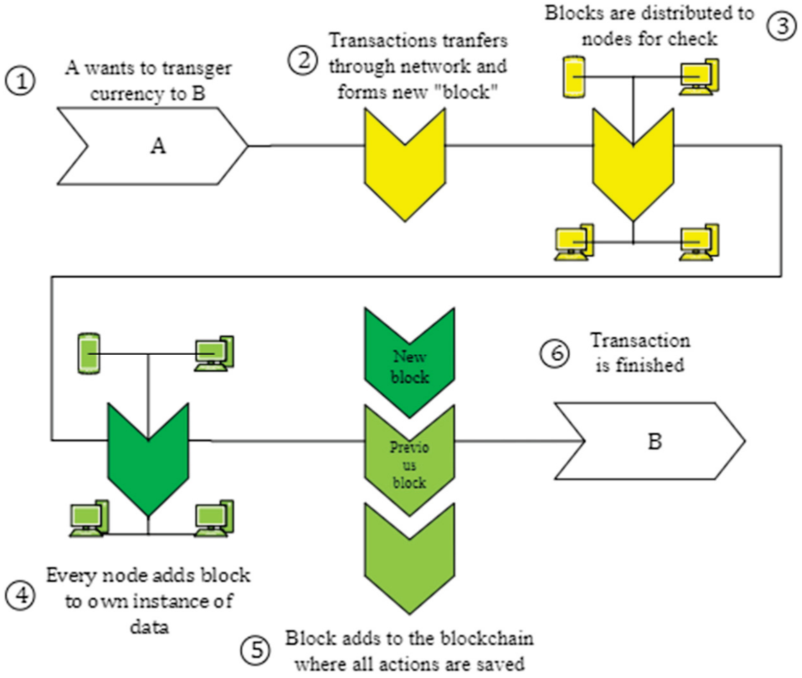

1
A wants to transger currency to B
A
2
Transactions tranfers through network and forms new "block"
Blocks are distributed to nodes for check
3
New block
Previo us block
6
Transaction is finished
B
4
Every node adds block to own instance of data
5
Block adds to the blockchain where all actions are saved

Figure 1. Blockchain processing diagram

At first glance, the system is very attractive, but there is another side. Privacy in the blockchain network protects users from hacking and preserves privacy, but also allows illegal trading and activity in the blockchain network. The most cited example of the use of blockchain for illegal transactions is perhaps Silk Road running on the DarkWeb, an online drug marketplace that operated from February 2011 until October 2013, when it was shut down by the FBI.

The website allowed users to browse the website without being tracked using the Tor browser and make illegal purchases in Bitcoin or other cryptocurrencies. Current US regulations require financial service providers to obtain information about their customers when they open an account, verify the identity of each customer, and verify that customers are not on any list of known or suspected terrorist organizations. This system can be considered both a plus and a minus. This gives everyone access to financial accounts but allows criminals to make transactions more easily. Many would argue that the good uses of cryptocurrency, like banking in the unbanked world, outweigh the bad uses of cryptocurrency.

2.2. Smart-contracts

Before considering NFTs themselves, it is worth paying attention to smart contracts, because they are at the heart of NFT processing. A smart contract is an application that runs on the Ethereum blockchain. It is a collection of code (its function) and data (its state) that resides at a specific address on the Ethereum blockchain.

Smart contracts are a type of Ethereum account. This means they have a balance, and they can send transactions over the network. However, they are not controlled by the user but are deployed on the network and run programmatically. User accounts can then interact with the smart contract by submitting transactions that perform the function defined by the smart contract. Smart contracts can define rules like a normal contract and apply them automatically using code [5].

Anyone can write a smart contract and deploy it on the network. You should know the language of contracts and have enough ETH to deploy your contract. Deploying a smart contract is technically a transaction, so you will have to pay for gas (fees) just like you would for a simple ETH transfer. However, gas costs for deploying contracts are much higher.

2.3. NFT

A non-fungible token (NFT) is a unique digital identifier that cannot be copied, replaced or split, recorded on the blockchain and used to prove authenticity and ownership.[6] Ownership of NFTs is recorded on the blockchain and can be transferred to the owner, allowing NFTs to be sold and traded. NFTs can be created by anyone and require little or no programming skills to create.[7] NFT occurs according to the reference of digital files such as photos, videos and audio. Because NFTs are uniquely identifiable assets, they are different from cryptocurrency, which is fungible.

The ERC-721 standard describes the general behavior of smart contract that can be considered as NFT and states that it must have a uint256 variable called *tokenId*, so for any ERC-721 Contract, the pair *contract address*, *uint256 tokenId* must be globally unique [8].

2.4. IPFS

Creating an NFT requires a repository where referenced media files in the blockchain metadata block will be stored. Such storage can be IPFS (Interplanetary File System) - a distributed system for storing and accessing files, websites, programs and data. IPFS knows how to find a file (HTML or media) by content, not location. Thus, instead of one request, for example, to one Wikipedia server "what is blockchain", a search will be made on many servers (computers) that may have this file. With IPFS, it's not just possible to download files from someone else, requesting computer also helps distribute them. If users’ friend on the same street needs the same Wikipedia page, he might as well get it from user or anyone else who uses IPFS.

IPFS makes this possible not only for web pages, but for any file a computer can store, whether it's a document, email, or even a database entry. Therefore, downloading a file from multiple locations has the following advantages:

- Supports resource availability. If someone attacks Wikipedia's web servers or an engineer at Wikipedia makes a big mistake that crashes their servers, pages can be retrieved from somewhere else.
- Makes content harder to censor. Because files on IPFS can come from many places, it's harder for anyone (whether states, corporations, or anyone else) to lock things down.
- Can speed up connection. If user can get a file from someone nearby, rather than hundreds or thousands of kilometers away, user can get it faster. This is especially important if community is locally networked but not properly connected to the wider Internet.

3. Cryptography in blockchain

3.1. General information

No part of the Ethereum protocol involves encryption, i.e., all communications with the Ethereum platform and between nodes (including transaction data) are not encrypted and can be read by anyone. It makes everyone capable of verifying the correctness and reaching a consensus.

There are two types of accounts in Ethereum: external accounts (EOA) and contracts. Ownership of EOA ether is established using digital private keys, Ethereum addresses, and digital signatures. Private keys underpin all user interactions with Ethereum. In fact, account addresses come from private keys: a private key uniquely identifies a single Ethereum address and from it as an account.

Private keys are not used in any way in the Ethereum system; they are never transmitted or stored on Ethereum. Private keys must remain private and never appear in messages transmitted over the network, nor must they be stored on the network, only account addresses and digital signatures are sent and stored in the Ethereum system.

3.2. Private key

The private key is simply a number chosen by chance. Ownership and control of the private key is at the root of user control over all assets associated with the corresponding Ethereum address, as well as access to contracts. A private key used to create signatures other than ether costs, proving ownership of the value used in the transaction. It is also necessary to create a backup copy of the private key and protect it from accidental loss. If lost, it cannot be recovered, and connected assets are also lost forever.

The first and initial step in key generation is to find a reliable source of entropy or randomness. Creating an Ethereum private key chooses a number between 1 and 2^256. The exact method used to select this number is irrelevant if it is unpredictable. Ethereum software uses the underlying operating system's random number generator to generate 256 random bits. A standard OS random number generator initializes the human source of randomness, so it may ask you to move your mouse for a few seconds or press random keys on your keyboard. An alternative can be cosmic radiation noise on the microphone channel of the computer.

More precisely, the private key can be any number between 1 and 2^256 - a huge 78-digit number, roughly 1.158*10^77. The exact number gives the first 38 digits of 2^256 and the series as the order of the elliptic curve used in Ethereum. To generate the private key, random 256-bit number must be selected and check that it is in a valid parameter. In programming terms, this is achieved by providing an even larger number of random bits (collected from a cryptographically secure source of randomness) in a 256-bit hash algorithm such as Kessack-256 or SHA-256, which can be used to produce a 256-bit number.

3.3. Public key

An Ethereum public key is a point on an elliptic curve, that is, a set of x and y coordinates that satisfy the elliptic curve equation.

To put it simply, an Ethereum public key is two numbers joined together. These numbers are derived from the private key through a calculation that can only go one way. This means that it is a trivial task to calculate the public key if you have the private key, but the private key cannot be calculated from the public key.

The public key is calculated from the private key using elliptic curve multiplication:

$$K = k * G \tag{1}$$

where: k is the private key, G is a fixed point called the generator point, K is the resulting public key, and is a special elliptic curve "multiplication" operator.

Elliptic curve multiplication is not like ordinary multiplication. It shares functional attributes with ordinary multiplication. For example, the inverse operation (which would be division for normal numbers) known as "discrete logarithm search" - that is, computing k if you know K - is as difficult a task as going through all possible values of k (brute-force - going through all possible combinations, step by step, cutting off already sorted values until the desired one is found).

Simplified: elliptic curve arithmetic is different from "regular" integral arithmetic. A point (G) can be multiplied by an integer (k) to get another point (K). But there is no such thing as division, so it is impossible to simply divide the public key K by the point G to calculate the private key k.

4. Proposed media file protection mechanism

4.1. Conception of protection mechanism

The figure 2 is presenting the algorithm of modern NFT buying and selling services.

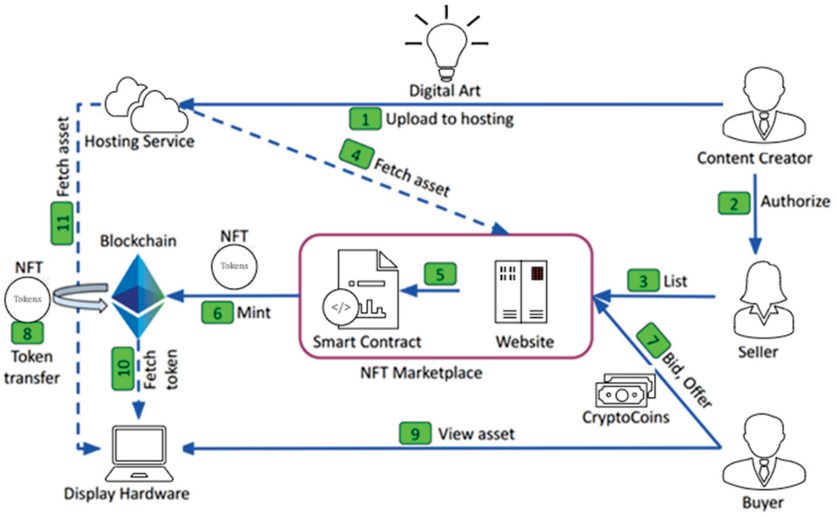


Figure 2. NFT marketplace workflow diagram

The algorithm has one drawback, the creator or author cannot control the process of creating NFT, similarly, the buyer blindly trusts the web platform in creating NFT. Therefore, when the Web platform is compromised, the NFT data can be permanently stolen. And this is one of the biggest disadvantages of this system, since the theft of tokens from exchanges or Web platforms occurs, although not often, but for very large amounts. In addition, it is the transparency of the auction, when attackers can see the formation of the amount for a specific NFT on the WEB platform, that increases the risk of hacking this platform. And, since the NFT is stored on the platform, this can be the reason for both hacking and reproduction of the "double" of the NFT by the platform's employees. Still, let's agree, to sell a painting for 12.5 million, and after a year or two to issue a "black double" NFT for some collector for a larger amount is a great bait for many platform workers.

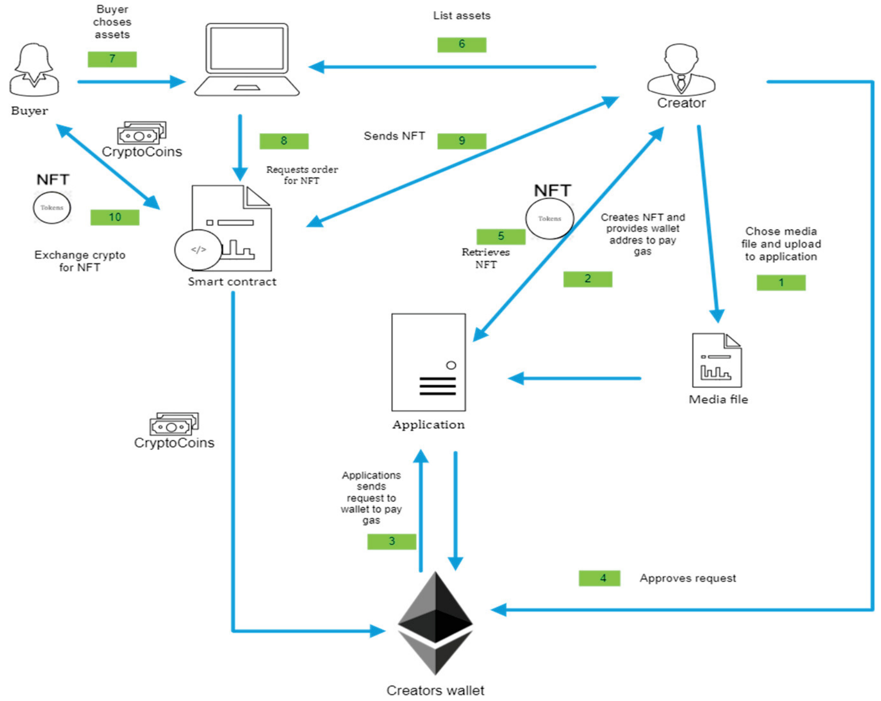


Figure 3. Diagram for proposed secure NFT creating application

In order to eliminate the corresponding vulnerabilities, it was decided to create an application with the help of which the author will be able to create NFT at any time and store it in his crypto wallet. (Fig. 3). In this case, the author protects himself from the hacking of the Web platform and the possibility of making a "black counterpart", since at the time of creation of the NFT, no one will know the amount for which this work of art can be sold. The creator keeps the NFT in his wallet until he wants to sell his creation. In this case, the demonstration can be held on any platform together with the auctions, and the purchase and sale are carried out directly through the Smart Contract between the seller and the buyer. The sales process is not shown in action, as this process is already implemented in many crypto exchanges, etc.

4.2. Implementation of proposed mechanism

The program will run locally using a non-public version of the blockchain, as each transaction is worth a certain fee. Node.js was chosen as the basis of the application because it has the NPM package manager, which allows to download and connect various libraries to the project [9]. This will give opportunity to initialize a Truffle project with basic settings for development. Truffle allows to get 10 wallets of 1000 ETH each in developer mode [10]. MetaMask is used as a wallet, which can be installed as an add-on to Google Chrome and Mozilla Firefox or as an add-on to a smartphone [11]. It also allows you to import local Ether wallets provided by Truffle. Pinata service will be used as IPFS [12]. The user logs in to the browser at localhost:8080 and connects the MetaMesk browser extension. Connects to the local blockchain and imports a Truffle account that holds 1000 ETH. The interface of the created application is demonstrated in figure 4.

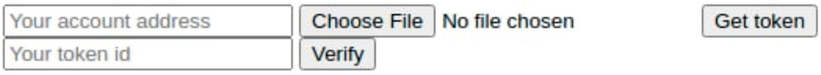
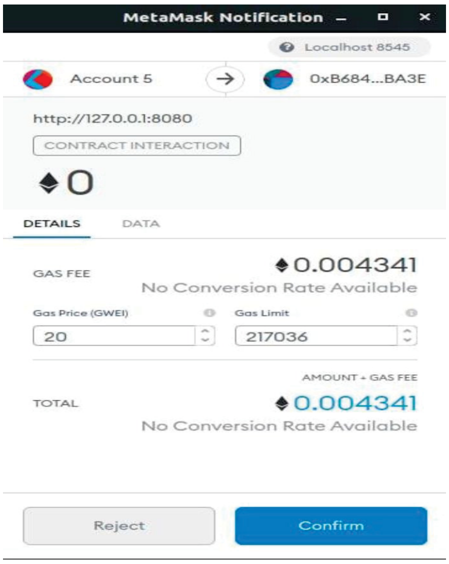


Figure 4. Interface of created application

The user enters his wallet address in the first input field, clicks the Choose File button and selects the file from which he wants to make NFT. For the transaction to go through, the user needs to click the "Get token" button and the application will generate NFT-token based on ERC-721 standard adding the wallet address as owner of the NFT, generate unique *tokenId* and contract address pair and upload media file to the Pinata IPFS to store it.



♦0

GAS FEE ♦0.004341
No Conversion Rate Available

Gas Price (GWEI) 20

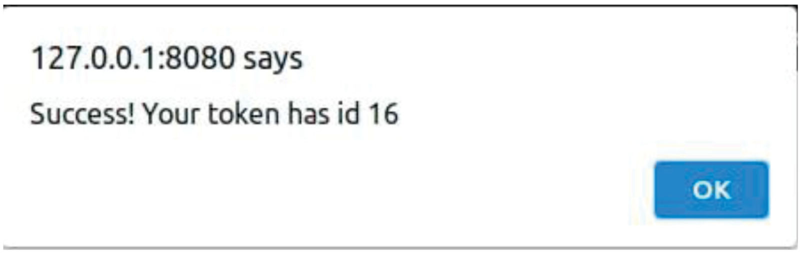
Gas Limit 217036

AMOUNT + GAS FEE

TOTAL ♦0.004341
No Conversion Rate Available

Figure 5. Confirmation of transaction

After confirming the operation, a message should appear that the transaction was successful, and the token was created and moved to the user's account (Fig. 6).

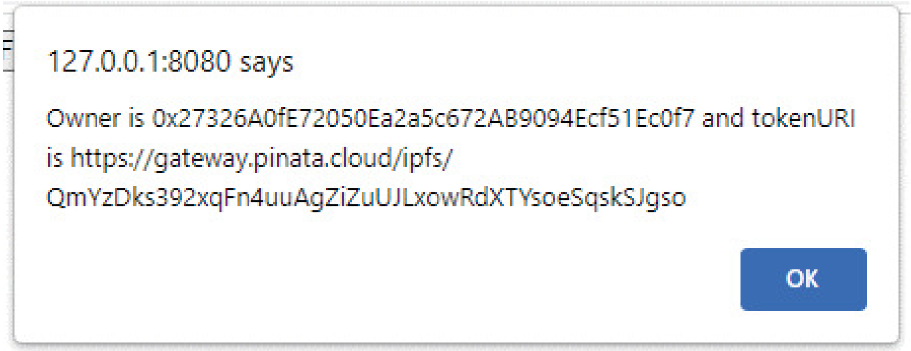


127.0.0.1:8080 says

Success! Your token has id 16

Figure 6. Successful operation

To make sure that the token exists in the blockchain and has a link to the media file, it is necessary to enter the unique identifier of the token in the input field and press the "Verify" button. As a result, the user receives a new message at the top of the screen, where it is written about who exactly is the owner of the token and what information this token stores (Fig. 7).

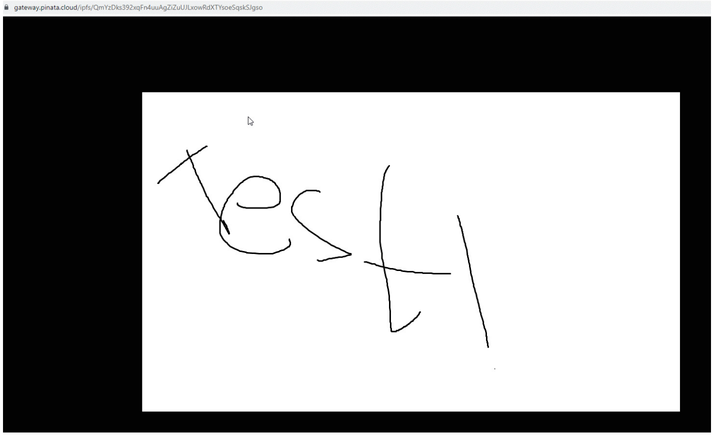


127.0.0.1:8080 says

Owner is 0x27326A0fE72050Ea2a5c672AB9094Ecf51Ec0f7 and tokenURI is https://gateway.pinata.cloud/ipfs/QmYzDks392xqFn4uuAgZiZuUJLxowRdXTYsoeSqskSJgso

Figure 7. Token check

The user can verify that their media file has been saved on the IFPS server by following the link. For example, a test media file was uploaded (Fig. 8). After following the link, the file that is under check is downloaded.



gateway.pinata.cloud/ipfs/QmYzDks392xqFn4uuAgZiZuUJLxowRdXTYsoeSqskSJgso

Figure 8. Uploaded file

4.3. Security recommendations for safe NFT storing

Enabling multi-factor authentication. The most important thing users should do to protect their NFTs is to enable multi-factor authentication (MFA). As the hacking statistics of various platforms in various industries show, attackers almost always steal money or data from users who do not use this feature. For example, in the Nifty Gateway hack described above, all victims had MFA disabled. The same can be said about the theft of money using phishing emails from Coinbase users. Moreover, consider using some authenticator applications or OTP instead of using SMS confirmation which is less secure [13].

Using a complex, long password. The benefits of a strong password, especially when combined with MFA, cannot be underestimated. Password must be of sufficient length and complexity that is not used by other accounts. It is best if it will be a set of random numbers and symbols that will be generated by some program like the one used in Google Chrome to automatically generate complex passwords when registering somewhere. This can be considered as strong password: *fmb#qD!64H4h* and this: *Password123* — cannot.

Keeping recovery phrase in a safe place. First, wallet passphrase must not be stored digitally. This means that no photos with smartphone can be take or saving them to a text file or save them on hard drive. It is also not worth saving it in an application for storing keys with passwords. All of these can be hacked or compromised, and NFTs will be lost. The best way to do this is to use paper or even titanium media (like CryptoTag.io) and use a storage method called RAID. It involves alternating information on three different hard disks, for example, if a file consists of three partitions, the first partition will be stored on the first hard disk, the second - on the second, the third - on the third. Of course, Seed phrase is best to store is use of paper and alternate words (Table 1).

Table 1. Example of storing Seed phrase.

Seed phrase		
Paper 1	Paper 2	Paper 3
The	-	The
Sun	Sun	-
-	Is	Is
Shining	Shining	-
Brigthly	-	Brigthly
For	For	-
Three	-	Three
Hours	Hours	-
-	Long	Long

Back up wallet regularly. It will help to easily restore data in the event of a system failure or device loss. A good idea is to create several backup copies and store them at once on 3 or 5 media, and it is best if one or two are external hard drives without connection to a computer and the Internet also this method is called “Cold wallet”.

Keeping software up to date. The most frequent software updates are security fixes. It is best to enable automatic updates of wallet, antivirus, operating system, mail client, and other programs.

Using of secure Internet connection. Using public Wi-Fi makes it easier for information to be stolen. So, if there is need to use public Wi-Fi, an encryption program and a VPN should be used always to secure your connection. Moreover, it's a good idea to turn on your device's invisibility and turn off Bluetooth.

5. Conclusion

Even though blockchain is a safe place for your NFTs there are still problems, which can let a cybercriminal hijack, forge or illegally use assets that he has no rights to. In this paper the NFTs marketplace is considered as the vulnerability to the security of creator's media files, as such marketplace have practice to store assets on their own hosting what can lead to data loss, hijacking, etc. Moreover, the fact of exposing assets to public can be a reason for cybercriminal to make decision that attack on the marketplace is worth based on data that are exposed as price for NFT, author, etc.

Considering fact that NFT marketplace can be compromised, and creator cannot know about this, or activity of the creator can lure the cybercriminal it is considered that the best way to store NFTs is store them on personal wallet that is disconnected from network.

In this work the conception of such method was proposed alongside with demonstration of the application that can create NFTs signatures for media files and store them on personals wallet, while uploading asset to the IPFS.

Also, recommendations of how store crypto wallet with created NFT safely were given. Moreover, such recommendations can be used to any other data that are needed to be stored securely.

REFERENCES

1. Sotheby's Is Selling the First NFT Ever Minted—and Bidding Starts at $100: *https://news.artnet.com/market/sothebys-is-hosting-its-first-curated-nft-sale-featuring-the-very-first-nft-ever-minted-1966003*, 20.10.2022.
2. NFTs Are the Biggest Internet Craze. Do They Work for Sneakers?: *https://www.wsj.com/articles/nfts-and-fashion-collectors-pay-big-money-for-virtual-sneakers-11615829266, 20.10.2022*
3. Atomichub: *https://atomichub.io/*, 20.10.2022.
4. NFT market worth $231B by 2030? Report projects big growth for sector: *https://cointelegraph.com/news/nft-market-worth-231b-by-2030-report-projects-big-growth-for-sector,* 21.10.2022.
5. Introduction to smart contracts: *https://ethereum.org/en/developers/docs/smart-contracts*, 21.10.2022.
6. NFT: *https://www.merriam-webster.com/dictionary/NFT*, 21.10.2022
7. How to Create an NFT – Simply Explained: https://eduwab.com/how-to-create-an-nft-simply-explained/, 21.10.2022
8. ERC-721 NON-FUNGIBLE TOKEN STANDARD: *https://ethereum.org/en/developers/docs/standards/tokens/erc-721/#top*, 21.10.200.
9. Node.js: *https://nodejs.org/*, 21.10.2022.
10. Truffle Suite: *https://trufflesuite.com/,* 21.10.2022.
11. The crypto wallet for Defi, Web3 Dapps and NFTs | MetaMask: *https://metamask.io/*, 21.10.2022.
12. Pinata | Your home for NFT media: *https://www.pinata.cloud/*, 21.10.2022.