Quick Answer: How to Protect and Secure the Use and Trading of NFTs

Published 25 May 2021 - ID G00752178 - 4 min read

By Analysts Avivah Litan

Initiatives: Applications and Software Engineering Leaders

Within a blockchain, a nonfungible token (NFT) represents a unique piece of digital media or a unique physical artifact. This research outlines how to decide terms for the utilization and trading of this new type of digital asset, which is often limited with regard to use and ownership.

Quick Answer

How can organizations protect and secure the use and trading of nonfungible tokens (NFTs)?

- Use distributed storage systems that support persistent storage and secure integration with blockchain networks.
- Utilize escrow services for NFTs: These services are especially needed when they are wrapped by other NFTs that add features to them.
- Purchase owner insurance to insure against the destruction or disappearance of NFT objects/files.
- Engage custody services that ensure safekeeping of NFT objects/files over time.

More Detail

When an organization buys an NFT, it gains the right to display the associated digital or physical object digitally, but does not own the object itself, unless such ownership is conferred in the end-user license agreement (EULA).

Users should pay particular attention to EULAs when they acquire NFTs. EULAs are rarely presented or signed, and sometimes the only link between the NFT smart contract and the object it points to is a URL. This means that the content stored at the URL can change without the owner knowing about it until after the fact. In most cases, the object and its metadata are stored separately from the purchased NFT because it is impractical and too costly to store the entire digital object on a blockchain.

The following analysis includes recommendations for protecting and securing the use and trading of NFTs, most of which are currently ERC-721 tokens on the Ethereum blockchain (although other blockchains also support NFTs).
NFT Markets Will Become More Transparent and Trustworthy

NFT buyers should demand to know where and how their NFT objects are stored. They can then make an informed decision about whether they can trust the NFT seller to provide persistent secure storage as long as they require it.

NFT sellers will eventually have many more easily accessible persistent storage options, and, over time, will likely start shifting ownership of storage to buyers. Buyers who want to keep their objects secure will be able to sign up for low-fee storage subscription services, much like Apple's iCloud storage service.

Points to Consider When Safeguarding NFT Metadata and Digital Objects

- Sellers should hash digital objects that reside off the blockchain network. A hash is essentially a digital signature or fingerprint for the content. (In the commonly used InterPlanetary File System [IPFS], hashes are called content identifiers [CIDs]). A hash should also be used to create the NFT that points to the hash in the off-chain storage system.
  - Most well-known brands that transact in or sell NFTs do this, so that anyone can validate a file/object's hash against the hash stored in the NFT, thus validating NFT ownership wherever the file/object resides.

- Many known brands store NFT-linked objects on their centralized servers, but this represents both a single point of potential failure and a single point of trust, which does not accord with the principles of democratized blockchains.
  - NFT file/object storage should, and often does, use a distributed file system, such as IPFS, and nodes should be replicated across many servers. This way, the system should be able to tolerate the disappearance of a single (or even a few) nodes that contain the NFT file/object.

- When using IPFS, the integrity of an NFT file/object depends on continual resolution of an IPFS file path to the blockchain, but some users report path failures (for examples, see Long Hierarchical IPFS Paths Fail to Resolve (HAMT, Object Links)).
  - Therefore, users should consider distributed storage systems like Filecoin and Pinata that offer persistent storage for a fee. Some, such as Filecoin, financially reward network contributors (see the Filecoin FAQ and Filecoin Mining Rewards).

- Buyers cannot assume that NFTs are legitimate just because they are cryptographically secured on a blockchain. There are already reports of “sleepminting” attacks — proven to work, at least theoretically — whereby NFTs are minted to a well-known user/artist wallet and then transferred to a hacker’s wallet without triggering any of the typical smart-contract security checks (see The Gray Market: How a Brazen Hack of That $69 Million Beeple Revealed the True Vulnerability of the NFT Market (and Other Insights)).
The growth of NFT commerce has generated many offshoot services, such as secure storage, escrow, insurance and custody services, that support the ecosystem for trading NFTs. These services are mainly offered by niche companies at present, but mainstream players such as insurance companies and banks will likely offer them in future to earn additional revenue.  

Figure 1: Top Five Blockchain Security Threat Vectors

1. **User:**
   - Weak private key
   - Password management
   - Weak endpoint security
   - Weak identity assurance
   **Risks:** User account takeover

2. **APIs, oracles**
   - Bugs, exploits, invalid data
   **Risks:** Incorrect smart contract execution, account takeover

3. **Off-chain and on-chain data:**
   - Unprotected data
   - Lack of data integrity, confidentiality
   **Risks:** Process failure, data compromise

4. **Smart contracts**
   - Bugs, exploits, unauthorized execution
   **Risks:** Theft, manipulation

5. **Permissioned nodes**
   - Insider threat, data exposure, dapp exposure
   **Risks:** Theft, manipulation, data compromise

Recommended by the Authors
Garbage In, Garbage Forever: Top 5 Blockchain Security Threats

Evidence

1 Examples of NFT escrow, insurance and custody services are, or can be found at:

- Cryptoexchange's NFT escrow services
- Insured.finance's decentralized digital asset insurance marketplace
- Hex Trust's digital asset custody services
- GeneralLiabilityInsure.com (NFT Insurance)