Atomic NFTs

IC3

Follow

The Initiative for CryptoCurrencies and Contracts (IC3)

--

Listen

Share

by James Austgen, Kushal Babel, Phil Daian, Ari Juels, and Mahimna Kelkar

In June of 2021, a group called PleasrDAO bought theDoge NFT for $4 million. The Doge NFT is a visual representation of a dog, a purebred Shiba Inu, shown below. This dog serves as the mascot for the joke-turned-multibillion-dollar-cryptocurrency that is Dogecoin.

On its website, PleasrDAO likens the Doge NFT in historical importance to the Mona Lisa. PleasrDAO's goal in purchasing it was to fractionalize

it, that is, subdivide control into shares so that ownership could be distributed across thousands of users.

About 20% of the Doge NFT shares have been auctioned off. At its peak, their market price implied a market capitalization of $225 million for the Doge NFT. (Today, it's of course muchlower.)

While the Doge NFT is perhaps the best known and most over-the-top example, the practice of NFT fractionalization has become widespread for high-value NFTs. There's certainly an argument to be made that fractionalization is beneficial: it democratizes ownership of art and collectables and can build communities of like-minded fans. In the case of the Doge NFT, for a fraction of a penny (exclusive of trading fees), anyone can in principle buy shares. Even you or I can join the club of owners of a digital asset that ranks among the most ludicrous and historically important in the world of crypto.

Why fractionalization may be undesirable

There are good reasons in some cases, however, for NFTs not

to be fractionalized. My group at Cornell Tech has spoken with artists who prefer that their works be owned by an individual aficionado and not be carved up as a commercialization strategy. Some financial firms we've spoken with, moreover, stress that NFTs are digital assets. They are concerned that fractionalization of NFTs can render ownership ambiguous or hard to trace, complicating regulatory compliance.

Is there therefore a way to prevent

fractionalization of a given NFT — or at least make it difficult?

Preventing fractionalization: A first attempt

NFTs reside in smart contracts — usually ERC-721 contracts.

Factionalization often makes use of a separate vault

smart contract to manage ownership: The NFT is locked in the vault contract, and ownership is then shared in some way, e.g., by distributing ownership tokens.

The contract in which an NFT resides can be modified so that the NFT can only be owned by an externally owned account

(EOA), i.e., an address that is not another smart contract. On the face of it, this approach would seem to rule out vault contracts and therefore prevent fractionalization of the NFT. As an externally owned account has a single

associated private key SK

, ownership of the NFT cannot involve a multiplicity of users.

There's a problem with this approach, though. It is possible to distribute control of a single key SK

itself among multiple users.

One way to distribute control of SK

is using trusted execution environments

(TEEs). A TEE is a tamper-proof hardware or software environment that can maintain confidential data and keys. (Examples include Intel Software Guard eXtensions (SGX) and Amazon Nitro enclaves.) A TEE can act like a trusted third party, adjudicating decisions — e.g., votes — by a set of owners. It can realize a fully functional DAO — again, in principle, without use of a smart contract. (Cryptographic techniques such as secret sharing

can achieve something similar.)

In short, a single key SK

can have multiple owners. No matter how a smart contract is constructed, it appears therefore that preventing NFT fractionalization is impossible.

Atomic NFTs

Despite the apparent impossibility, we have devised a technique of constructing NFTs so that they cannot easily be fractionalized — even using tools such as TEEs. We refer to NFTs constructed using our techniques as Atomic NFTs

.

Realizing Atomic NFTs involves a small change to the standard (ERC-721) contract for NFTs. Normally, in any smart contract, transactions such as transfers and sales of digital assets are authorized using conventional digital signatures. For instance, to sell an NFT owned by an account with secret key SK

requires a transaction signed using SK

.

An Atomic NFT contract, however, authorizes transactions using a new cryptographic protocol. This protocol has the property that to generate a signature using SK

, someone

must be able to learn SK

. It is not possible for SK

to exist only in hidden form, tucked away for instance in a TEE. This property means that there can be no safe fractionalization of the NFT controlled by SK

. There's always someone

who can learn SK and

take complete control of the NFT if she so chooses.

The details of this new form of signature are in a forthcoming paper with Vitalik Buterin of the Ethereum Foundation on a concept called Complete Knowledge (CK)

. To give some intuition, though, one variant involves storing SK

in a TEE. (Yes, we use a TEE to prevent fractionalization by another TEE.) The TEE spits out a key

SK locally to the user

when it uses the key to generate a signature. Some user therefore can learn SK

. (Another variant based on proof-of-work (POW) uses off-the-shelf cryptocurrency mining hardware to complete the protocol.)

We have created an Atomic NFT contract and minted a few trial Atomic NFTs with accompanying visuals, shown below. We plan to showcase them at the IC3 NFT Gallery Opening on 3 Oct.

In summary

Atomic NFTs introduce new cryptographic techniques in order to enable NFT creators to prevent fractionalization of their NFTs. Our work promises to give creators stronger control over how their NFTs are bought and sold.

We stress that Atomic NFTs are a preliminary research concept. More research needs to be done to make them truly practical. We believe, however, that practicality is on the horizon and that Atomic NFTs could someday become a standard option in NFT creation.