A Year Embedded in the Crypto-NFT Space: From Digital Ownership to Artistic Communities

In December 2021 my university's press office asked if I could answer some questions from newspapers on the Crypto-NFT phenomenon which was getting a lot of public attention then (prices were going up). I knew a bit but felt that it was not enough, so I had to decline, but then decided I wanted to know more of the actual scene and not just the high-level concepts behind consensus, byzantine fault tolerance, and such.

I created a new Twitter persona and started following some accounts in that space. Had to learn the ropes behind creating crypto wallets; writing down the sequence of words that serve as mnemonic to the deterministic generation of your key pairs and wallet addresses (see BIP39); and authenticating myself in the sites via wallet, usually by scanning QR Codes.

It is a lot of technical setups, done by regular users when gearing up to use these Web 3.0 technologies. It would not be surprising that some users just follow the recipes and have no insight into what is happening underneath and what are the security tradeoffs in some choices.

Consider the specific case of the Ethereum blockchain, where the public key is generated from the private key under elliptic curve cryptography. The first step is to generate the private key, possibly seeded from the word list, and then the public key. This should occur in a device that is hard to be compromised. It can be a dedicated hardware device, like a ledger, or just any machine that can be properly secured. In the Ethereum blockchain, accounts are identified by wallet addresses that are derived from the public key by a hash function. Initially, those addresses have 0 funds, in this case, Ethereum currency $ETH. Any account holders (controlling their private keys) can transfer funds from their accounts into other accounts. One way to convince them to transfer into your new account is to pay them with regular money. That is what Exchanges do (e.g. Coinbase and Binance), they are regular sites in Web 2.0 that interface with credit card providers and regular banks and allow trading fiat currency into cryptocurrency.

Another way to increase the balance in an account is to convince another account to "voluntarily" transfer into it. Bad actors do this by compromising the secrecy of the private keys (if you know the key or the word list, you also control the account) or by hijacking someone's computer data and coercing the victim to transfer the currency. This is the dark side of anonymity.

During the crypto rise of 2017/2018 most of the action revolved around new blockchains and cryptocurrency tokens, traded as commodities. The distributed systems community also started contributing more to the theory supporting blockchains, such as the fundamentals behind swapping assets among different blockchains and understanding the actual deployment of popular systems.

Non-Fungible Tokens

Like the money in a bank account, cryptocurrency tokens are fungible. Once you receive some amount it gets added to your balance and cannot be distinguished from any amount that was already there. However, other use cases require distinct entities and identities. A distributed ledger, implemented by a blockchain, can easily support registers that hold a new unique non-fungible entity, i.e. a non-fungible token (NFT), associated with some metadata (e.g. a small image or some text). The transfer mechanism can be tweaked to keep track of the initial owner (the one initially minting the NFT) and process changes of ownership among wallets, mimicking the trade of physical objects.

In some way, this tries to provide a mechanism for providing some form of ownership of digital assets. But "owning" NFTs is not as obvious as it might seem, see a quote from an article on The Verge: "Copyright law does not give an NFT owner any rights unless the creator takes affirmative steps to make sure that it does — ideally, by executing a standard, formal copyright license to the work connected to the NFT."

Not surprisingly, the creator and owner of the work (and let's assume that the owner is the same entity that uploaded and minted the NFT) is the one who can control how much licensing is granted to future NFT owners. Even simple things like printing them or displaying them in an exhibition should not be taken for granted.

Most NFT owners are also probably unaware when buying any sizeable NFT with non-trivial metadata, such as a photograph or a painting, that the picture itself is not stored on-chain. Typically, what is stored is a link to a website or an access key to a P2P system that is dedicated to content storage, such as IPFS. When linking to websites, more often than not, no content checksum is stored in the metadata. This means that the piece can simply disappear or be replaced by something else (see a metadata example on opensea.io).

While it might be questionable if the current "owner" of an NFT was even given rights to display it, since many NFTs are not explicit on the licensing granted to them, it is also true that the owner of the work had to adhere to some licensing terms when uploading it. For instance, on objk.com, a popular platform for creating and trading NFTs on the Tezos blockchain, uploading content confers a license "to access, use, host, cache, store, copy, reproduce, transmit, display, publish, distribute, adapt ..." and specifies how these rights are transferable. Since these sites have the right to host URLs with the content, the NFT owner can at least know that he or she also can access them, as well as all other users while the content is online.

PFPs, vanity and utility

Although the origins of NFTs can be traced to earlier dates, the CryptoPunks NFT profile pictures (PFP) on the Ethereum chain became a very influential project after its launch in 2017. Some years later, these pixelated pictures of punks reached prices equal to a small family house.

A non-initiated can rightfully wonder how this valuation could be reached. The answer is probably tied to rarity and fame. Items that exist in small supply and, for some reason, become famous can increase significantly in value. Our history is rich in examples of items

whose utility is dubious apart from the fact that they are exclusive and expensive, see Fabergé egg. Surprisingly, for items with few perceived common-sense usefulness, in some projects, expensive NFTs are given *utility* by conferring the owner special privileges, either by acting as membership cards for events or by giving discounted access to other NFTs to be launched. In 2022 Twitter added the possibility of using your owned NFTs as a specially framed profile picture, further highlighting (or dooming) the status of the account. In games, NFTs can be used to grant access to specific items or act as proof of ownership for in-game real estate.

In most of these use cases, NFTs are presented as collections of items. This helps bring visibility and liquidity to the projects. After the initial successes and high valuations, countless projects are being created with new collections and pitched to buyers as the next big lottery ticket. Often, they don't shoot to the stars and eventually get forgotten. Still, there is a lot of excitement inside the Discord chats with the hope that *we all gonna make it* (WAGMI), and some *fear of missing out* (FOMO) on the next big valuation. For a full lexicon check this guide to NFT terminology.

A bright corner

Far from the spotlights of the top collections of NFTs, there is a small but vibrant art corner where artists create and sell to collectors, which often are other artists. One can't avoid finding parallels to all the artistic experimentation that brewed in Paris at the turn of the 20th century. Here one can find 1-of-1 pieces, where a creator mints a single edition piece and auctions it to potential buyers. Again, there is an expectation of future valuation, but a collector can focus on pieces whose aesthetic value to herself matches the price. Personal collections can be arranged on 3D NFT galleries and navigated in a browser or in a VR Headset, a striking experience (one of my favourites is Keepcase's gallery at OnCyber.io).

In real-world settings, an artist usually has little control over a piece that was already sold. Banksy's shredded artwork is a good example of exerting some control over secondary sales. With NFTs, the underlying smart contract technology that regulates transfers of ownership allows for interesting new mechanics. The original artist can stipulate when minting, the intended share of future secondary sales, say 10%, and proceeds automatically get transferred into the minting account upon each sale. Other mechanisms could be devised, like sharing profits among sellers and gallery curators.

After little more than a year of a journey in this space and subculture, my impression remains ambivalent. On one hand, there is a high share of Ponzi schemes and deception, but there is also a small community of artists using the technology to connect with their audience and regain some control. Only time will tell if this is a fad or a way forward.

Acknowledgements

I would like to thank Paulo S. Almeida and Rui M. Abreu for their comments on improving this text.

Carlos Baquero is a professor in the Department of Informatics Engineering within the Faculty of Engineering at Portugal's Porto University and also is affiliated with INESC TEC. His research is focused on distributed systems and algorithms.