City Research Online

City St George's, University of London

Citation: Alonso, E. & Mondragón, E. (2024). NFTs 101. In: Bonadio, E. & Sganga, C. (Eds.), NFTs, Creativity and the Law: Within and Beyond Copyright. (pp. 1-19). Milton Park, UK: Routledge. ISBN 9781032497402 doi: 10.4324/9781003395508-1

This is the accepted version of the paper.

This version of the publication may differ from the final published version. To cite this item please consult the publisher's version.

Permanent repository link: https://openaccess.city.ac.uk/id/eprint/36875/

Link to published version: https://doi.org/10.4324/9781003395508-1

Copyright and Reuse: Copyright and Moral Rights remain with the author(s) and/or copyright holders. Copies of full items can be used for personal research or study, educational, or not-for-profit purposes without prior permission or charge, unless otherwise indicated, provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way. For full details of reuse please refer to City Research Online policy.

City Research Online: http://openaccess.city.ac.uk/ publications@citystgeorges.ac.uk

NFTs 101:
Non-Fungible Tokens and the blockchain may not be what you think

Eduardo Alonso and Esther Mondragón
Artificial Intelligence Research Centre (CitAI)
School of Science & Technology
City, University of London, London, UK

Abstract Non-Fungible Tokens (NFTs) and the blockchain are a relatively new technology that is becoming ubiquitous –yet most creators and buyers are saturated with an ever-increasing arsenal of jargon that, in some cases, makes it difficult to fully appreciate what exactly an NFT is and how the blockchain really works and, thus, to comprehend what is being sold and bought and which rights the players are entitled to. This chapter serves two purposes, namely, to introduce the main technical concepts underlying NFTs and the blockchain in layman's terms, and to set the *mise-en-scène* for the rest of the chapters of the compilation.

Keywords Non-fungible tokens; blockchain; consensus mechanism; smart contract; asymmetric encryption

1 Introduction

In the sections that follow we will describe NFTs, clarifying some misconceptions about the uniqueness, and associated value, of non-fungibles, and their relationship with the assets they represent "in real life" (IRL). Next, we will explain the distinction between the internet and the blockchain, that is, between distributed and decentralized networks, and how such differences affect their governance. We shall continue with a gentle exposition of the main consensus mechanisms (Power of Work and Power of Stake), and how they tackle issues of security and scalability. In this journey, familiar concepts such as minting, mining, hash values, double spending, crypto wallets, and the Byzantine Generals problem, among others, will be introduced with simple examples. We will highlight such terms as they appear in the text in bold, for ease of reference. Finally, some controversies surrounding the blockchain will be summarily examined.

But, before we start, it is necessary to state some disclaimers: First, due to the speed at which the blockchain evolves certain technical specifications covered in this chapter may become outdated quickly; yet the main principles should remain the same. Second, and relatedly, exposition will be intentionally high-level, giving enough detail for non-experts to understand the basics of how the blockchain operates without the need to become a specialist in distributed computing systems or cryptography. Third, there are many ways of illustrating the fundamental concepts involved in the blockchain and NFTs –in this narrative glossary, we will use examples from NFTs in the art-world, because it is the art market where the blockchain has penetrated with more impetus,[1] and because NFT art provides us with visual scenarios that people naturally understand. Finally, although this chapter is factual in that it is intended to explain the main practical aspects of a technology, the blockchain, the reader will find references to philosophical essays that may help framing its impact in a more general, cultural context.

[1] *See* Mekacher et al. (2022).

As a closing comment, it must be acknowledged that this book is the result of the contributions to the "Copyright Encounters with the Blockchain, NFTs and AI Creativity" workshop organised at City, University of London the 13th of September 2022 and supported by the Alan Turing Institute through a Turing Network Development Award.

2 Non-Fungible Tokens

To explain what **NFTs** are, we will first describe what a "token" is, and delineate why tokens are essential for the functioning of the blockchain and partly responsible for the misunderstandings surrounding it –specifically, in reference to the relationship between the token that lives in the blockchain and the reality, for instance, a digital image, the token represents outside the blockchain; then, we will analyse their non-fungible character, which has been, in turn, deeply misinterpreted.

First, from a semiotic point of view a **token** is a representation of something else, a signifier. Why do we use tokens in the blockchain and not the corresponding assets they represent directly? Because, in the blockchain, keeping copies of the originals will be computationally too expensive. The reasoning is similar to why gamblers use tokens of one-thousand pounds in a casino: if they were to use real one-pound coins, the table will overflow quickly, making playing the roulette impractical. Thus, they use tokens instead. What makes a token non-fungible? **Non-fungible** means that the token cannot be exchanged because it is unique. Of course, everything can be exchanged for something else, but a fungible token can be exchanged for another undistinguishable token of the same kind. If you borrow some sugar from me, I am not expecting you to return me the same sugar. Sugar is fungible. However, if you take care of my cat Felix while I am on holidays, I will definitely expect you to return Felix to me, not another cat. Felix is non-fungible (NF), it is unique.

It is a common misconception though to conclude that NFs are valuable because they are unique. Such mistake refers to the historical argument of scarcity: in a digital world where art is freely reproduced, mixed, and shuffled a million times through the internet, artists were struggling to find a way to add value to their creations, to monetize on them. NFTs presented a potential solution to such conundrum, since they are unique, and thus scarce. We are told that an NFT is unique in that it is a unique digital signature, a unique alphanumeric code in the blockchain. But let's look at it more closely: a lottery ticket is also unique (all natural numbers are unique!) and, at least before the draw (and ignoring the fact that some people attach magical powers to specific ciphers, like their daughter's birthday), they are fungible. In fact, in some countries people exchange lottery tickets as a sign of friendship. One ticket, one unique number, is the same as another. So, the value is not in uniqueness –you can exchange unique yet fungible tokens. In conclusion: *an asset is not NF because it is unique; rather, it is unique because it is NF.* Hence, if the unique data signature that identifies the token does not make it an NFT, what does it?

Let's try to answer this question looking at a well-known example in postmodern art: Imagine that you are presented with the two pictures in Figure 1. One is Walker Evan's *Alabama Tenant Farmer Wife*, 1936; the other, Sherrie Levine's famous appropriation, *After Walker Evans: 4*, 1981. Now, without the signature(s) you won't be able to know which one is the original and which one is the copy, that is, they will be fungible, interchangeable. In fact, the two pictures could be copies of Evan's work, or of Levine's. What makes them unique, both, are their signatures –as, you might argue, the digital signature of an NFT is. So, we are back to square one. Now, the

signature, "*Walker Evan, Alabama Tenant Farmer Wife, 1936*" is just an alphanumeric sequence. Granted, in the blockchain a digital signature is truly unique, in that nobody can reproduce it (more on the technical details later), unlike Evan's signature, that can be easily forged; yet the point is that the value doesn't lie in the sequence of characters as such but rather in the artistic and exchange value assigned by the art-world to such signature. In fact, the photographs will come with their corresponding certificates proving ownership and provenance. This should not be so strange: there are billions of footballs, yet one signed by Messi will have more value than any other football. It is the signature what makes that particular ball valuable, but only in so much as we attached vale to Messi, as with Picasso's cheques. Pablo Picasso used to pay even the most trivial goods and services by cheque, knowing that the cheque, as a container of his signature, will be more valuable than the amount on it.

Figure 1. Believe it or not, these pictures are not the same work of art. Each is unique. (Sources: https://www.artsy.net/artwork/walker-evans-tenant-farmers-wife-alabama-1 and https://www.xavierhufkens.com/artworks/after-walker-evans-4, in no particular order).

Let's look now at Figure 2, depicting the work of crypto-artist Josie. They appear to be identical, so they should be fungible. However, their tokens in the blockchain are unique, and non-fungible. In the blockchain, we don't even see the pictures the tokens are linked to (which may not even exist). In the blockchain, we see unique datapoints. Again, unique datapoints are not valuable in themselves. These are special datapoints in that they certify ownership in the blockchain as a verified transaction. The evidence of ownership is what makes them valuable (not their physical or digital uniqueness) and what buyers are after. That's why a tokenized "copy" in the blockchain costs millions and the same non-tokenized "copy" moves freely on the internet. In short: *an NFT makes a fungible token non-fungible*.

This may look surprising, but it merely reproduces in the virtual world how the art market works in the real world.[2] Collectors buy art in auctions by phone, without even seeing the pieces. When they buy a Cattelan or one of Manzoni's cans they buy the right to brag, and because they know it is good investment. A flourishing NFT market is "real" estate (see, for instance, Decentraland): (rich) people buy virtual NFT mansions. What for? What's the value of a virtual mansion? You cannot live in it, not yet at least. But the same applies to real mansions. I doubt that David Beckham has

[2] *See* Thompson (2012).

even the time to walk through all the rooms of his mansions, he has probably not even visited some of his properties. It doesn't matter, because, in his social class, mansions or yachts are just symbols of wealth, and a good investment.

Figure 2. Josie's Choose #3 and Choose #4 (Source: You can see a colour version at https://andrewsteinwold.substack.com/p/the-history-of-non-fungible-tokens).

Technically, an NFT is a unique alphanumeric sequence generated by a crypto function. The NFT lives in the blockchain, and it encrypts information about an asset including a link to the asset that lives, itself, off the blockchain. That is, the asset (*e.g.*, an artwork) the NFT is a token of is stored outside the blockchain. The intriguing thing is that, whereas the NFT is unique, the asset might not: The "real" artwork can change, be replicated, or become unavailable. This is what I coin as the "*reverse Dorian Gray effect*". Whereas in Oscar Wilde's play the "virtual", the portrait, decays with time, the "real", Dorian Gray, remains young and "healthy" (he is insane, of course). In the world of the blockchain, it is the "virtual", the NFT, what remains immutable, whereas the "real" changes. In that respect, the situation is more factual than the literary counterpart. The point is that when you buy an NFT you are not buying the signified, only the signifier; you are not buying the "real" artworld, but the unique, digital signature of a transaction. This reminds us of *Zone de Sensibilité Picturale Immatérielle*: between 1959 and 1962, Yves Klein sold eight certificates of ownership of empty space, in exchange for gold; the "piece of art" could then be completed in a performative act in which the buyer would burn the receipt, and Klein would throw half of the gold into the Seine in the presence of an art critic or dealer, and an art museum director.

In short, it is costly to store an image or video clip inside a token. The NFT contains metadata about the asset, a description of the artwork, a file name, and an URL address. If you follow the address, you will be directed to a website (typically off-chain, *e.g.*, in the InterPlanetary File System, IPFS) where the artwork is stored … presumably. The crucial fact is nevertheless that the token is NF whereas the asset may be fungible. The blockchain becomes a self-contained world, in which value is not attached to the provenance of the asset the NFT refers to, but to the provenance of the NFT itself through transactions recorded in the blockchain. The asset may lose value as the NFT increases it. In other words, the token generates value through circulation, a nice example of "the medium is the message" aphorism:[3] the blockchain, as a

[3] *See* McLuhan (1964).

medium, creates new messages independently of the content, which, in fact, deteriorates through dispersion –as anticipated in by Seth Price.[4]

Why is this relevant for the present book? Because it is important that those selling and buying through the blockchain understand what they are entitled to. Perhaps paradoxically, the lack of an actual relationship between NFTs as assets and the assets they represent outside the blockchain, is reflected in the rights of NFT owners and of the owners of the assets. Those who don't own the NFT are still able to access the artwork and the rightsholder is free to continue providing it, selling it, or otherwise distributing it to the public. Owning an NFT, by itself, doesn't grant one the right to print or distribute the work without the copyright holder's permission. This is doubly so if the artist didn't authorize the NFT in the first place. Despite such caveats, artists have been appealed to "mint" NFTs, why? Because in the blockchain where NFTs are transacted over, artists have complete control over pricing and their customer's data, fees are lower than dealers' commissions, they can benefit from a percentage on secondary sales, and they can continue to capitalize on the physical artwork, that is, they can try different business models. In short, and this is where we started, the blockchain does give the artist a way to manage the distribution and monetization of their art, to break with mainstream art and its gatekeepers –in principle, as we will see next.

But, before proceeding to describe the main technical concepts underlying the blockchain, we would like to finish this section on NFTs on a positive note. The exposition so far may strike the reader as overtly cynical, exposing the use and abuse of NFTs as a speculative means of making money, rather than of expressing artistic creativity. You may reach the same conclusion if you only pay attention to CryptoPunks and Bored Apes. Let's be clear: this is not the case. Considering art as the practice of disclosing meaning in an alienated, technological world,[5] artists have used NFTs to counter the dominating consumerist narrative. Perhaps one of the most cited examples is Anna Ridler's work, *Bloemenveiling*, 2019 (Figure 3).

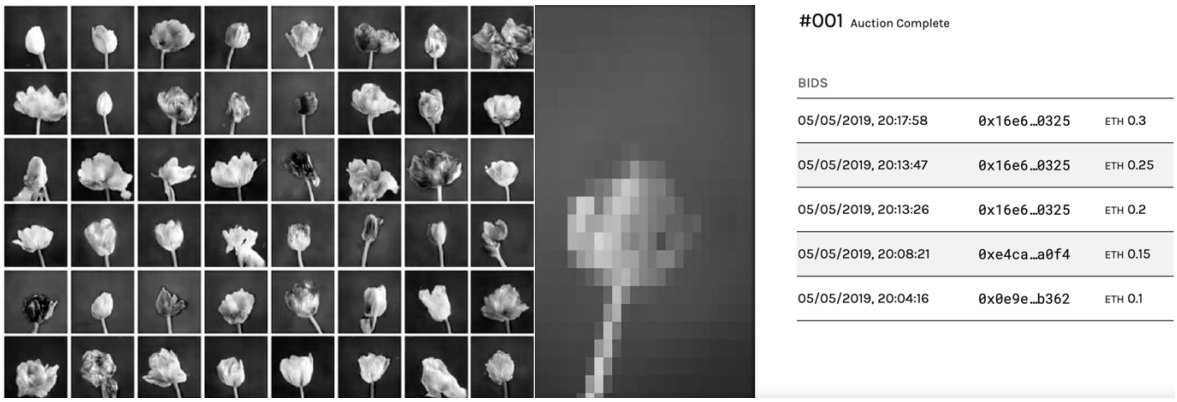

Figure 3. Anna Ridler's work. Left, images of tulips created by AI, in *Mosaic Virus* (Source: colour version at http://annaridler.com/mosaic-virus); right, a unique *Bloemenveiling* auctioned token (Source: colour version at http://annaridler.com/bloemenveiling).

In this work, Ridler explored the way the blockchain creates scarcity of assets that can be unrestrictedly generated using Artificial Intelligence (in particular, Generative

[4] *See* Price (2002).
[5] *See* Heidegger (1954).

Adversarial Networks, GANs[6]). Infinite images could be produced (as in *Mosaic Virus*, 2018, Figure 3, left), but the ones that are valuable are those that are associated with a finite supply of NFTs (Figure 3, right). To reveal the commodification inherent to the blockchain, Ridler chose images of tulips in reference to the tulipmania, a period during the Dutch Golden Age when bulbs were not bought or sold as physical objects but rather as paper contracts – as NFTs are in the blockchain. A perhaps more dramatic example of artivism denouncing the NFT market is Banksy's *I Can't Believe You Morons Actually Buy This Shit*, 2007: the anonymous street artist burned the original artwork, but first turned it into a NFT that was sold at Christie's in 2019 for $32,500.

3 The blockchain

Remember the good old internet days? For (digital) artists it came with all sorts of promises, an explosion of net.art and surf clubs, and the works of pioneers like jodi, Cory Arcangel, Vuk Ćosić and Olia Lialina.[7] It was the time of New Media Art and institutional critique, where the emphasis moved from the aura of the unique creation of the heroic artist to understanding art as a participatory, multimedia activity. It allowed artists to avoid gatekeepers and offered them freedom to distribute and monetize their work independently as politized prosumers of a progressive mass culture, fulfilling Walter Benjamin's prophecy.[8] However, it became clear very soon that the internet was not the panacea, as the technology pessimistics Max Horkheimer and Theodor Adorno would have predicted.[9] The internet works with centralized client-server protocols, and the servers where data (personal data, bank accounts and transactions) is stored are privately owned; paradoxically, in principle, any node can request access to and duplicate a file – and without scarcity, artists cannot capitalize. The blockchain came to the rescue: while the internet is, with some caveats, the highway of information, the blockchain is the highway of value. The **blockchain** is a truly decentralized system, where all nodes act as servers and as clients. It contains data grouped into blocks concatenated in chronological order, a temporal chain, of which all nodes have a copy. That all nodes have a copy of the data guarantees **transparency**, but it comes with a price: it would be far too (computationally and financially) expensive to keep multiple copies of digital assets such as images of music files; hence, the need to tokenize them. In other words, NFTs are stored in the blockchain because there is no other space "big" enough to accommodate the assets they represent and to secure true decentralization at the same time.

One may wonder though, how is it possible to be unique, and to create value by scarcity, when all nodes have a copy of the blockchain? That all nodes have a copy, in

---

[6] GANs are AI models that consist of two artificial neural networks, one that generates images, the generator, and another, the discriminator, that tries to classify examples as either real (from the domain) or fake (generated). The two models are trained together in an adversarial zero-sum game, until the discriminator model is fooled, meaning the generator model is generating plausible examples. GANs were used by the art collective Obvious in producing *Edmond de Belamy*, which was sold at Christie's for $432,500 in 2018, news that caused furore in the artworld and the AI community alike. AI art brings its own IP issues, as the piece *85.81%_match: Amel Chamandy 'Your World Without Paper', 2009* shows: *see* Zeilinger (2021). Who is the author, the AI that generates the artwork or the human artist that designs the "experiments" and curates production? Are the authors of the images used to train the GANs or to automatically assess AI's artistry entitled to compensation?

[7] *See* Paul (2015).

[8] *See* Benjamin (1935).

[9] *See* Horkheimer and Adorno (1947).

real time, of the blockchain means that anyone can check whether it has been altered "illegally", for example, one node claiming ownership of an NFT for which there is no validated, traceable transaction record. There is nothing unique about the NFT other than as a certificate of ownership *in the blockchain*. That any node has access to a duplicate of such certificate does not alter its uniqueness. It is as if you were to check the title deeds of a property using the HM Land Registry's online service. You can download it (copy it in your own computer) if you wish, but you cannot change it or claim that you own the certificate of ownership (and thus the property attached to it). That is because the uniqueness of the certificate rests on its belonging to a validated, traceable chain of documents/transactions (in this case owned and managed centrally, by the UK Government, but this is not relevant). The same happens with digital art: anyone can make copies of it, but only one can claim ownership; and this is what the NFT certifies within the blockchain validation system.

Before entering the technical aspects of the blockchain, let's recapitulate on NFTs. As said, an NFT is a digital signature (a certificate of ownership), which takes the form of an encrypted **hash** –and it is such encryption what makes it unique. In simple terms, a mathematical function called "hash" transforms any input data into a compact 256-bit, unique code, randomly. As a result, similar inputs produce very different values (Figure 4). Although the function is random in the assignment of hash values, it is nevertheless deterministic in that the same input gives the same output –so, it is easy to verify, knowing the input and the function. But it is one-way, so you cannot retrieve the input from the output.

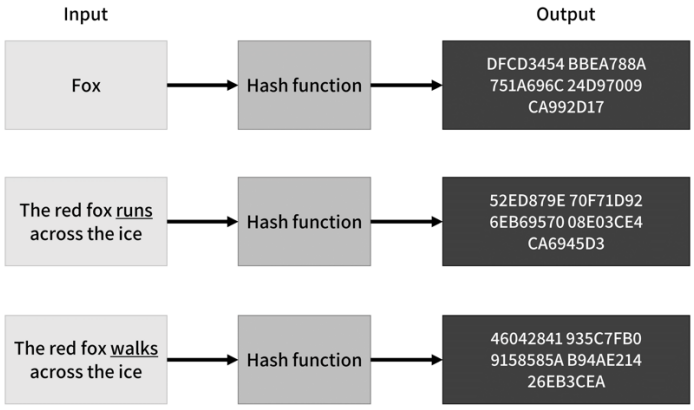

Figure 4. A "hash" function creates unique crypto code. In the blockchain, an NFT whose input is the metadata of the asset.

The blockchain is a digital ledger of transactions (of NFTs and other tokens like cryptocurrencies) that is duplicated and distributed across the entire network of computer systems (on the blockchain). Transactions are time-stamped and stored in sequences (chains) of blocks of information, concatenated by the hash values of previous blocks of transactions (Figure 5).

Now, how does the blockchain work in practice? The main issue is to keep the balance between **Decentralization, Security and Scalability** (the **DSS balance**). Let's explain each in more detail. As we have seen, the main difference between the internet and the blockchain is that, whereas the internet distributes resources it does centralize governance. The blockchain, on the other, is truly decentralized, and thus it requires **consensus mechanisms** that incentivize nodes to build (validate

transactions) and manage it. Such decentralized approach has consequences with regards to security. When you spend five pounds IRL, you "lose" five pounds (they are not in your wallet anymore, you cannot spend them again). In the digital world, however, what prevents you from spending cryptocurrency twice? You could hack the blockchain and put money back into your crypto wallet. This is what we call the **double spending problem**.

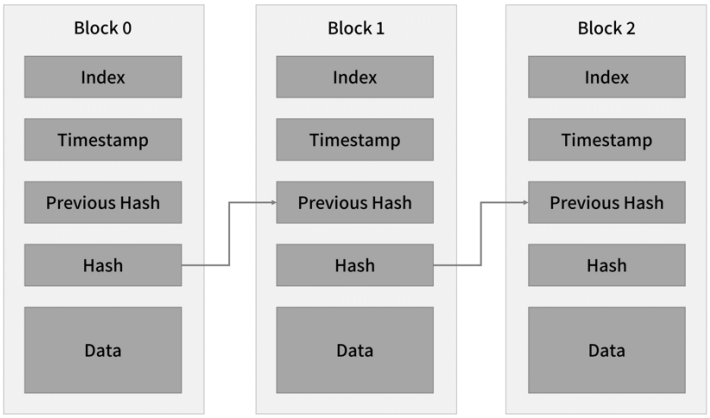

Figure 5. The blockchain: Blocks of transactions chained by hash.

One consensus mechanism that avoids such scenario is **Proof of Work (PoW)**, (still) the most common consensus mechanism, also known as **mining**. In PoW, every node has access to a transaction and competes to validate it and add it to a block (to the blockchain). These will be the ones who solve first a computational problem, namely, to find a hash value close to a target (called the "difficulty") using a nonce (number only used once) repeatedly on the hash of the previous block. Minting is thus down to the brute power required to execute a computationally expensive automatic task, not about developing sophisticated algorithms that solve complicated mathematical puzzles –as it is typically and misleadingly described. The first node "solving" the task, gets a reward over the expense they incur, that is, nodes trade electricity for rewards; they lose everything if they cheat. Remember that whereas it is difficult to solve the problem, it is easy to verify whether the result is valid. For some problems, there is no way to find an answer quickly, but if we are shown the answer, we can verify it quickly. In computing *parlance*, the validation problem is in NP (the class of problems that are quickly checkable in nondeterministic polynomial time) but not in P (quickly solvable). Or, using a mundane example, any solution to a Sudoku game is easily verified, and the time to verify a solution increases polynomially (slowly) in relation to the size of the grid. However, finding a solution to the same game takes time that grows exponentially as the grid gets bigger.[10] Remember that the very essence of a hash function is that it makes it easy to verify that a given set of data is the same as the original set of transactions, but not to obtain the original set of transactions.

PoW is, in principle, decentralized. Note, however, that the power needed to validate transactions favours the formation of pools and farms of ASICs, which

[10] As COVID-19 infection curves.

monopolize and potentially control the blockchain, for example, creating forks.[11] This refers to the **51% attack** security problem: If some nodes manage to control 51% of the blockchain, they will be able to do as they please. It is not easy, though.

A combination of hash and asymmetric cryptography (explained in the next section) makes PoWs secure: To change a transaction, you need to break the hash of the transaction and not just in one block but in the whole blockchain, hash over hash. This refers to another characteristic of the blockchain, its **immutability**. Nobody should be able to tamper with the content of the blockchain (and double their coins). To get a clearer picture of the magnitude of the task, notice that we do not run the entire block of transaction data through the hash function. Rather, each transaction is hashed, then each pair of transactions is concatenated and hashed together, and so on until there is one hash for the entire block.[12] Visualized, as in Figure 6, this structure resembles a (co-called Merkle) tree. Note that the image is highly simplified; an average block contains over 500 transactions. Then consider that the "final" hash of the block is chained to the hash of previous blocks in the blockchain (as in Figure 5).

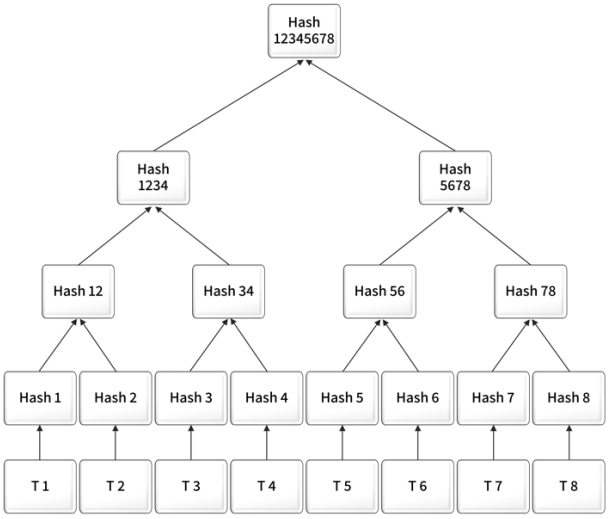

Figure 6. A Merkle tree of hashes in a single block of transactions, where "T" designates a transaction.

PoW is thus decentralized and, to some extent, secure. But it is scalable? No, it is not. It takes around 10 minutes to create a new block depending on the "difficulty" of the validation task (which is, in turn, updated every 2,016 blocks).

A different consensus mechanism that is becoming popular is **Proof of Stake (PoS)**. In PoS, not everybody can validate, rather the transactions are split in what is called **sharding**, and allocated randomly to nodes (known as forgers, not miners) proportionally to their stake. "Stake" is the crypto coins they "invest" and that put in reserve during validation. If their validation is verified, the get their stake back plus a fee (on the value of the transactions); they lose their stake otherwise. Since computation (validation) is split, it is more scalable and less expensive than PoW. It is still secure and decentralized in that transactions are allocated randomly, so nodes

[11] Miners don't use standard computers, they use chips designed for the purpose, so called Application-Specific Integrated Circuits, AISCs.

[12] If there is an odd number of transactions, one transaction is doubled, and its hash is concatenated with itself.

don't have an incentive to try and control the blockchain. The forgers don't know who will be validating which shard; plus, the transactions they validate in a shard may not be related to each other.

Notwithstanding the importance of the DSS balance and how it is tackled in different consensus mechanisms (and there are dozens of them), what is common to all is that they act as programmable payment rails where work and payment happen automatically and are united. This is seen as a huge advantage over traditional payment systems that require all sorts of permissions and checkpoints and allows experimenting with new business models that are sustainable and interoperable.

4 I want to sell my NFT in a blockchain: Quick guide

In order to explain other aspects of the blockchain (and NFTs), let's imagine that you are a digital artist, and have your work stored on the internet so that it can be retrieved from a virtual address once sold.[13] This work is not an NFT yet.

Your digital art will be sold through a **marketplace** or platform (*e.g.*, OpenSea, Foundation, Rarible, or SuperRare, just to mention a few) in a blockchain, for instance, Ethereum.[14] So, you need to open an account in the platform. Also, you need a way to be paid once your work is sold; and you will also need to pay a transaction fee, called the **gas fee**. So, you must link your bank account to a **crypto wallet** (*e.g.*, Coinbase or MetaMask), where you transfer real money into its corresponding crypto value. Such wallet is also connected to the blockchain. In fact, the cryptocurrency is not stored in the wallet –crypto coins are just numbers that exist in the transactions you are involved in on the blockchain. It is like with your (virtual) bank account, where digits come in and out. What is stored in the wallet are **keys** or passwords that you will need to execute transactions securely. In fact, such wallets are more like key holders than wallets. As IRL, you need to keep your keys safe. You may decide to keep them on the internet, in so-called hot wallets, which is fine but vulnerable; or you can write them in a piece of paper and lock them in your drawer, or you can use an USB. The latter are called cold wallets. Crucially, keys come in pairs, public and private, which are complementary and used to encrypt and to decrypt messages (transactions identifying addresses where the coins are stored).

Now, you upload your art in the marketplace along with a description of the work and the address from which it can be retrieved, what is called the metadata of the NFT. By doing so, you create (**mint**) your NFT. Only that it is still not an NFT as such. The corresponding NFT will be a unique number, the result of hashing all that information. This operation is not executed on its own, but rather as part of a transaction that takes the form of a **smart contract**. Such transactions are themselves hashed and stocked in blocks of transactions that are then chained. You know the drill by now.

The marketplace consists of a web front end where products are advertised (**listed**), and the selling takes place. It also connects to the digital wallets (of the buyer and the seller) and to the external data storage service where the work is located, and executes the smart contracts (through a Web3 API) that, in turn, refer to transactions in the blockchain.

---

[13] The IPFS is a common storage internet service, where information is accessed by content. This is ingenuous, since it prevents work being "lost" when addresses change or become unavailable.

[14] Notice that Ethereum is a blockchain, not just a cryptocurrency; in addition, the Ethereum Request for Comments is the most popular blockchain standard, including ERC-721 for NFTs; fortunately, the programming language used to implement contracts in the Ethereum blockchain is called Solidity!

You can sell for a fixed price for an unlimited duration or offer the NFT at a gradually reducing price. Alternatively, offers can be submitted through an auction, Dutch or English, with a reserve price. Once a deal has been agreed on, it is executed as a smart contract. Such smart contracts are neither smart nor contracts. They are not smart because the underling code is implemented automatically. They are if-then rules that follow the paradigm "code is law". As such, they have been compared with vending machines: you insert a coin and, automatically, without intermediaries, get the goods you are buying. More importantly perhaps, there is no legal context for such blockchain contracts, hence their legality and, again, whether they are actual contracts, is questionable. But I leave this debate to the IP lawyers that contribute to this volume.

That smart contracts are mechanised leads us to a controversial characteristic of the blockchain, namely, its **trustlessness**. How can we advocate a system that is not worthy of trust? In human interactions, trust is essential. In art, you trust fellow artists, collectives, and communities; and you trust your dealers and gallerists; you must trust your customers as well. Or you may not and decide that you would rather interact with them through automated exchanges. Whereas this may be one of the original reasons behind the blockchain (artists becoming suspicious of their agents), trustlessness responds in fact to a technical requirement. In (complex) distributed systems there is no guarantee that communication and thus consensus be faultless. This is called the **Byzantine Generals Problem** –that describes a situation in which the actors must agree on a concerted strategy but can't because there is no guarantee that all of them are reliable (there may be traitors or a malfunctioning server). In other words, in truly decentralized systems, trust cannot be trusted. This can go against our philanthropic impulses, but it is a technical fact. In the blockchain, trust is replaced by processes that make it unnecessary –consensus mechanisms and automatic smart contracts. Or, in other words, we deposit our trust in trustful protocols that are not going to fail us. We trust code because it does what it says on the tin. As we trust the law of gravity.

This is where the keys in the wallet become important. How can I get paid safely? and how do I know that my counterpart is really who they claim they are? You need to make sure that the message is secure, and that the identity of the messengers is correct. This is where **asymmetric encryption** (aka public key cryptography) comes in, which involves two keys, one public, that everybody knows, and another private, that only a given person has access to and that is linked to their public key. Let' see how they work in a simple, conventional scenario: Imagine Bob trying to send a message (moving money from one account to another) as part of a transaction to Alice. Alice and Bob have each their public-private keys. What if Bob uses his public key to encode the message? If a hacker intercepts it, they won't be able to decode it, since only Bob has the corresponding private key. So, it looks like a secure means. The problem is that Alice doesn't have Bob's private key either. So, a sender using their own public key is a safe but useless way of communication. You can argue that Bob could have sent his private key to Alice in advance, but that's precisely the point: the private key could always be intercepted by a third party. The trick is to encode the message with Alice's public key, which everybody has access to, but that can only be decoded with Alice's private key, which only she has access to, as in Figure 7. Clever!

Now, how do we make sure that the sender is indeed who they say they are? This is where **digital signatures** come in. To reassure Alice that Bob has sent the message, Bob encrypts the message using his own private key. On receipt, Alice can verify that Bob is the sender of the message using Bob's public key. This may seem counterintuitive, given the explanation of asymmetric encryption above, but, in this case, we just want to ensure the identity of the sender: If you encrypt something with

your private key, anyone can decrypt it, but this serves as proof that you encrypted it: it is "digitally signed" by you.

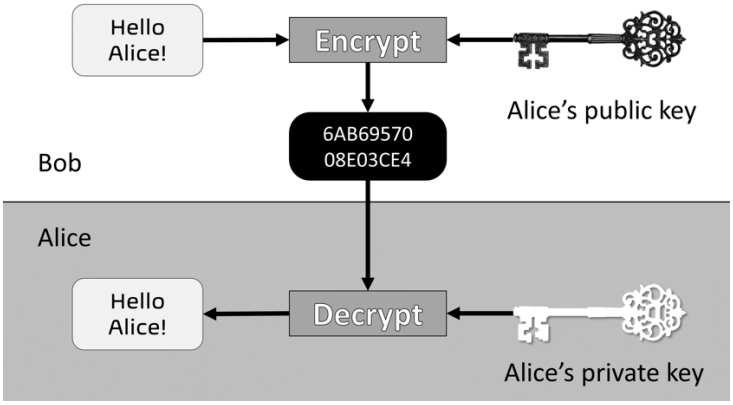

Figure 7. Asymmetric encryption.

How do digital signatures and asymmetric encryption work together? Let's explain it using an analogy with boxes and blocks: If Bob wants to send an encrypted message to Alice, and only Alice should be able to both decrypt the message and verify the identity of the sender, he will have to first put the message in a box and put a lock on the box, and then lock the box using his own private key. He will then put the (locked) box in a new box and put a new lock on the box. He will lock the new lock using Alice's public key. After Bob is done, he sends the box to Alice. Once Alice receives the box she can open the outer box with her private key, and the inner box with Bob's public key. Who said that cryptography was boring?

5 Conclusions

Despite the potential benefits of the blockchain, namely, transparency, decentralization, and security, and that NFTs create scarcity and value that users can monetize directly on, we must not forget that it is an emerging and experimental technology and thus caution in assessing and adopting it is advised.

In the blockchain there is still human validation, from communities and marketplaces (some of which apply quite strict entry requirements and high fees). Rather than putting the effort in securing a good gallery, you must put it into being accepted by peers in a **Decentralized Autonomous Organization** (DAO) and doing your own (massive) representation in different fora (Telegram, Discord) and social media. This leads to hyperproduction and hyperconsumption. In fact, DAOs don't necessarily guarantee democratization either, as the case of Hic et Nunc (HEN, 2021) proves;[15] examples abound nevertheless of their utility in realising self-governance and in bringing together communities in artistic, urban, and environmental projects.[16]

Decentralization is more an idea than a reality in practice. There is not a blockchain, there are blockchains –that can be used by different platforms and DAOs

[15] *See* HEN at: < https://matheussiq8.medium.com/hic-et-nunc-the-story-facts-suppositions-and-ideas-june-2021-19927f9106ad > (accessed 30 December 2022).
[16] *See* Catlow et al. (2017).

under different conditions of membership and payments. Importantly, most blockchains delegate certain functionalities to decentralized applications (**dapps**) or Layer 2 blockchains, which, in turn, may not follow a decentralized approach strictly.

That in the blockchain the price of cryptocurrencies (with which NFTs are eventually paid) fluctuates due to the number of people using the network rather than being dictated by a central authority is a double-edged sword: on the one hand, it is a self-regulated way of controlling value that cannot be tampered with by governments or corporations; on the other, it is a very volatile system, suited for speculation.

On the concept of trust, it has been argued that centralized systems, though looked at with reservations by some, are actually trusted by most people. We may disagree with the Bank of England when interest rates increase, yet we don't mistrust the institution as such –rather we see it as an independent guarantor of good financial practice. We don't lose our sleep pondering whether our money is safe in the bank or about the possibility of deeds on our house being suddenly deregistered either. In addition, we continuously give free access to our personal data to all sorts of companies and organizations. It is debatable whether, in so doing, we are simply the victims of disciplinary power as Michael Foucault might put it;[17] on the other hand, the blockchain is presented as liberating, and yet it implements a (lack of) metanarrative that considers humans and their interactions as transactional tokens that can be owned and exchanged, that is, as quantified commodities ready to be managed scientifically in terms of performativity.[18] In other words, is the blockchain really "the internet we want"?[19], an internet that channels democratic interventions?.[20]

With regards to immutability, it is worth refreshing our memory: The first public DAO was launched the 30th of April 2016. In less than a month it became the largest crowd-funding exercise in history, raising over $160M. On June 17th it was hacked using a (simple) recursive call attack. Apart from questioning the security of the system, a debate raised on whether the blockchain should indeed be immutable. Failures eventually happen, either provoked by untrustworthy agents or because trustworthy agents make honest mistakes in designing and coding the blockchain. In such cases, should we not amend the record of transactions "to make it right"?

There is of course, the ecological issue: the blockchain infrastructure is powered by electricity, which is mainly produced by fossil fuels that account for 64% of the world's electricity. A single transaction costs an average of 82 kWh, with emissions of around or 48 kg of CO2. On average, the expense of a single issue is equivalent to driving a gasoline car for 1,000 kilometres.[21] Some blockchain fans counterargue, cynically in my view, that running a real-life transaction system is not ecological either –banks also use computational power and electricity in physical premises, not to mention intercontinental flights to close important agreements.

Relatedly, the fact that building the blockchain is computationally expensive is reflected in how slow it runs –although, in most cases, the user won't notice the time difference between a payment done via the blockchain or a centralized system like a credit card.

Finally, since art is one of the markets that has embraced NFTs more fervently, it is worth considering their impact in terms of art theory and practice. NFTs may in fact

---

[17] *See* Foucault (1975).
[18] *See* Lyotard (1979).
[19] *See* Stlieger (2017).
[20] *See* Feenberg (2017).
[21] *See* Akten (2022).

be "reactionary": with ready-mades, art became information, and information is public; NFTs, on the other hand, make information private.[22]

To conclude, we have seen the potential consequences that the dichotomy between the blockchain and the "real world" may bring. However, for the blockchain to make sense, we need to understand it as a self-contained system. It is not about signifiers and signifieds anymore. All tokens in the blockchain are signifiers that refer to themselves, confirmation of Jean Baudrillard's hyper-reality.[23] This may seem wrong, to assign value to a meaningless cipher, but it is the world proposed by the blockchain. Armed with this understanding, it is your decision to enter it and explore its possibilities, for instance, in the future metaverse or to reject it as a scam. Either way, we encourage the reader to keep an open mind about new technologies: photography was considered as the "death of art", before being adopted as a valid creative tool in its own right; equally as importantly, photography liberated painting from its attachment to representation and mimics, opening the path to impressionism and cubism, to modernism and postmodernism. Can you imagine a world without Henri-Cartier Bresson, Tina Modotti, Shirin Neshat, and Andreas Gursky? without Paul Cézanne, Wassily Kandinsky, Faith Ringgold, and Helen Frankenthaler?

References

Akten M (2022) The Unreasonable Ecological Cost of CryptoArt. https://memoakten.medium.com/the-unreasonable-ecological-cost-of-cryptoart-2221d3eb2053. Accessed 23 December 2022

Baudrillard J (first published 1981) Simulacra and Simulation. Glaser SF translator, University of Michigan Press, Ann Arbor: MI (1994)

Benjamin W (first published 1935) The Work of Art in the Age of Mechanical Reproduction. Underwood JA translator, Penguin Books, London (2008)

Catlow R et al (2017) Artists Re:Thinking the Blockchain (eds). Torque Editions & Furtherfield

Feenberg A (2017) Technosystem: The Social Life of Reason. Harvard University Press, Cambridge: MA

Foucault M (first published 1975) Discipline and Punish: The Birth of the Prison. Sheridan A translator, Penguin Classics, London (2020)

Heidegger M (first published 1954) The Question Concerning Technology. In: Krell DF (ed) Basic Writings: Heidegger. Routledge, London (2nd ed, 2010)

Horkheimer M, Adorno T (first published 1947) Dialectic of Enlightenment. Cumming J translator, Verso Books, London (2016)

Joselit D (2021) NFTs, or the Readymade Reversed. October 175: 3–4

Lyotard J-F (first published 1979) The Postmodern Condition: A Report on Knowledge. Bennington G and Massumi B translators, Manchester University Press, Manchester (1984)

McLuhan M (first published 1964) Understanding Media: The Extensions of Man. Routledge, London (2001)

Mekacher A et al (2022) Heterogeneous Rarity Patterns Drive Price Dynamics in NFT Collections. Scientific Reports 12:13890

Paul C (2015) Digital Art. Thames and Hudson Ltd, London (3rd ed)

Price S (2002) Dispersion. http://www.distributedhistory.com/Dispersion2007.comp.pdf. Accessed 23 December 2022

Stiegler B (2017), La Toile que Nous Voulons (ed), FYP Editions

[22] *See* Joselit (2021).
[23] *See* Baudrillard (1981).

Thompson D (2012) The $12 Million Stuffed Shark: The Curious Economics of Contemporary Art. Aurum Press Ltd, London
Zeilinger M (2021) Tactical Entanglements: AI Art, Creative Agency, and the Limits of Intellectual Property. Meson press, Lüneburg