9

Playtime: Monitoring and Surveillance in NFT Sociality

Matan Shapiro

Introduction

A networking event was held in a London pub. I arrived early and started talking with Laura, the organizer, about exciting new business opportunities in cryptocurrency investment. Then, a middle-aged woman arrived. She introduced herself as 'Angie', and after a brief chat tried to convince us to invest a few hundreds of pounds in what she defined as a 'blockchain investment' that will yield tens of thousands in return. Laura answered bluntly that the offer sounded like an invitation into a pyramid scheme. Angie insisted that it was legitimate, nonetheless. More people arrived in the meantime, and we were all caught up in other conversations. Angie stayed in the pub for another 30 minutes, pitching her lines and writing up some contact numbers. When she finally left the pub, Laura approached me. 'That woman was a typical scammer', she determined. 'These people never stay until the end. They try to collect emails and phone numbers so they can follow up the next day. That's how they work, *and they are wasting our time*'. When I inquired further what 'wasting time' meant in this context, Laura said:

> There are artists here trying to promote their digital art and explore new ways to making money. All these scammers put up a good show so it's difficult to know who to trust and from whom you should stay away. If you find out [that] you were trying to make a partnership with someone who is not honest you just ended up wasting your time.

Laura was right to suspect Angie. In 2021 more than $3 billion was stolen from cryptocurrency exchange platforms or from individuals using them, with overall security breaches rising more than 40 per cent *every year* since the first major cryptocurrency theft took place in 2011 (Derrick, 2021). In 2022 millions of dollars were also stolen in different non-fungible token (NFT) swindles, including three major fraudulent schemes related to the once-prestigious lifestyle brand 'Bored Apes Yacht Club' in April and May 2002. The ever-present possibility of fraud in this social landscape assigns a ghostly mystique to the figure of the 'scammer', who could appear suddenly in your inbox using the email address of your best friend, or might even turn out to be a middle-aged woman you accidently met in a pub.

In this chapter I will focus on Laura's and other self-defined 'honest' traders' perceptions of timelessness, loss of time, or 'waste' of time, which they associate with the ongoing requirement to identify potential 'scammers'. Rather than analyse these ideas as pertaining to a rational risk aversion strategy, I examine them as forms of play, which create a suspension of everyday economic calculations, while introducing a measure of uncertainty into nearly every encounter with other traders, online or offline. NFT playtime in fact *replaces* the 'Big Motherly' monitoring of mundane economic rhythms (Peacock, Introduction, this volume), consequently generating the temporal precision of new economic and political rhythms (see Thompson, 1967; also Peacock, Introduction, and Polan, Chapter 10, both this volume). Based on fieldwork I conducted in 2022 with NFT traders and collectors in London, I advance the assumption that play theory may shed new light on the contemporary expansion of surveillance online, which is becoming ubiquitous not only in blockchain-related social circles but also other digital milieus.

NFTs

In October 2008, a person or group of people using the pseudonym Satoshi Nakamoto, in a cryptography mailing list, published an academic paper titled 'Bitcoin: A Peer-to-Peer Electronic Cash System' (Nakamoto, 2008). Satoshi, as cryptocurrency investors (especially Bitcoin adopters) have come to call them, described a decentralized system for the production of electronic money that innovatively solved what programmers and game theory experts call 'the problem of double spending' online. The solution reliably enabled peers to send and receive digital tokens, while ensuring that: (1) there is no fear of duplication (sending the same token twice); and (2) there is no need to go through a 'trusted third party' (Nakamoto, 2008), such as banks, to audit and guarantee the authenticity of the transaction.

Satoshi called this system 'the blockchain', an automated digital ledger in which every 'peer' holds a copy of the entire history of transactions. The blockchain thus registers all transactions between peers in real time, while verifying which of these transactions is fraudulent and which is honest. At the same time, using an algorithmic process called 'mining' (Zimmer, 2017), the blockchain also produces a set number of digital tokens that are released back into the network to produce value.[1] Every 10 minutes, the system seals this data in a virtual 'block', which contains a detailed record of all the transactions that were registered in the last 10 minutes on the ledger, *as well as* the details of the single computer that 'solved' the encrypted riddle from which the new coins were created. Every such 'block' is then assigned with a time-stamp sealing, which cannot be altered because it is protected by a cryptographic formula that makes it effectively tamper-proof (Antonopolous 2016). The signed block is immediately linked to the block that preceded it, which is already linked to the previous block, thus generating a 'chain' of verified blocks that stretches diachronically all the way back to the first block ever produced on the relevant blockchain. While Satoshi's blockchain produces only one type of digital tokens – the infamous Bitcoin – later blockchains could handle other cryptocurrencies, and in recent years also began monitoring the transactions of entirely different sets of decentralized tokens, such as NFTs.

NFTs, as their name suggests, are digital tokens whose storage on the blockchain turns them into tradeable goods or assets, much like Bitcoin and other cryptocurrencies. These tokens can be image files, music files, video files, or any other type of file which the creator/owner would like to register as theirs. Many NFTs are stored on the Ethereum blockchain – currently the main network used for the trade and exchange of cryptographic digital assets – but there are other existing blockchains that host NFTs. All these networks transparently show the different owners each NFT has had from the moment it was created and posted online (in a process similar to 'mining', which is called 'minting'), along with their changing prices through time. This enables all peers on the network to track the trajectory and value transformations of each NFT ever posted. Meanwhile, the cryptographic code assigned to each individual NFT guarantees its authenticity as a 'one-of-a-kind' item. Each NFT can then become an object for commodification, its value derived from the sums of money people are willing to pay for owning it. Since each NFT is singular and unique, it cannot be exchanged for other NFTs. While cryptocurrencies are all the same (or 'fungible', meaning that any single bitcoin is fully identical with any other bitcoin), NFTs can only be bought for the price tag that their owner has set in advance, whether that price is designated in cryptographic money or in state-owned fiat money.

For example, imagine you created a beautiful picture of a cactus on your digital drawing pad, and you now wish to make a profit by selling it online to cactus enthusiasts. The process is fairly simple – first, you create a digital wallet for yourself, which is essentially a hub, or a postal address, used exclusively for sending and receiving money online. Access to the wallet is exclusively yours, and is protected by a personal password that only you can change. Then, you will be able to connect your wallet to a blockchain of your choice (for example, Ethereum); each blockchain has different advantages and challenges, including varying transaction and storage fees, which means that some form of comparison is required if you wish to reduce the overall costs. Once that is done, you can link your wallet address to any of the many NFT marketplaces online (for example, OpenSea, Rarible, or NBA Top Shot), and upload to this marketplace the file you wish to sell. The file is then presented online side by side with graphs and other information regarding its trading and ownership history. Since NFTs represent ownership or proof of authenticity of a unique item, they can also be used to designate membership in a community, ownership of virtual or physical property (for example, land or a house), celebrity and lifestyle symbols, brand development and marketing, purchasable icons in the gaming industry, or any other object that requires nominal legal singularity and whose value can be derived from its scarcity (or rarity).

NFTs are not, however, attractive merely due to their potential financial value. Many of the traders and collectors I met in different public meetups in London or online were merely experimenting with this new form of digital asset 'for fun'. There are currently many online self-described NFT 'communities' and forums where collectors interact, including physical meetups or drinking nights. On the Discord network, for example, NFT enthusiasts engage in conversations on diverse issues, ranging from new 'hot mints' recently available on the market, to warning about 'scams', selling tickets to or publicizing information about related events, and NFT-related news in the gaming industry. Likewise, NFT communities hold digital art contests, exhibitions, and online treasure-hunt games aimed at finding and winning NFTs on different platforms (much like a *Pokémon Go!* game). In 2023, these have been expanded to include prestigious Web3 and metaverse events or parties,[2] which bring together creators, technologists, and entrepreneurs to chat, foster partnerships, and make friends, meeting in a random pub online using avatars. While there is an underlying economic value to these engagements, most of the time they fall under the category of play, as I now outline.

Play in NFT sociality

Since the 1950s, scholarly analyses of play have shifted the theoretical focus from a view of play as a 'free' activity (Huizinga, 1970 [1939]), to a view of play as a communicational vehicle in the ongoing negotiation and transformation of social values (Caillois, 2001 [1961]). When people reach a tacit understanding, 'This is Play' (Bateson, 2000 [1972], pp 177–193), they establish a communicational framework that is structurally separated from non-play events (Caillois, 2001 [1961], Handelman, 2021). The term 'framework' refers here to the implicit understanding that actions during playtime are *not* subjected to the same moral judgements and normative interpretations that non-play actions would require (Bateson, 2000 [1972]). For example, if during play I 'shoot' my playmate and she 'dies', I might have to accept some form of reaction or sanction within the rules of the game – whatever they are – but nobody will think of calling the police, and any sanction will dissolve after the game is over. If my playmate *really* dies, however, the moral and legal weight of everyday life will take over the play scenario and I will most likely go to prison, even if the tragedy was an accident. Playfulness thus allows persons to experiment with types of symbolic interaction that expand the possibilities of everyday non-play conduct, but this can rarely fully replace non-play resonances and real-world consequences.

The temporality of play thus suspends reality while not entirely ignoring the boundaries, conventions, norms, and rules that usually govern the flow of mundane life (Stromberg, 2009). This temporal bracketing, which enables participants to frame their activity as playful, accompanies several structural components (Huizinga, 1970 [1939]). These are: (1) people engage in play freely, rather than being coerced into it; (2) a clearly defined set of rules or norms constitutes an acknowledged playful order, which must be accepted by all the participants for the play or game to be considered effective or 'fun'; (3) when play activities become productive, especially with regards to the creation of wealth, they become instead a form of labour. Roger Caillois (2001 [1961]) argues that this set of structured characteristics contains four main types of human playful activities. He uses Greek terms to classify them as (1) *agon* (competition); (2) *alea* (chance, luck); (3) mimicry (make-believe, role-playing, imitation); and (4) *ilinx* (often translated to English as 'whirlpool' and referring to the sense of losing control over one's body or cognition).[3]

The world of NFT investors is playful in at least three aspects. To begin with, NFTs are a type of collectibles, much like traditional hobbies that include the collection of stamps, artworks, stickers, old swords, and so on. Collection and trade in NFTs include elements of *agon* (competition) and *alea* (chance), much like financial edgework activity that involves speculation and risk (for example, stock exchange investment; see Smith, 1999; Borch 2007). Although notions of profit do form part of this activity, NFT trade is rarely undertaken as a main source of income or a 'job', pertaining more to the realm of 'leisure' or 'hobby', as an interlocutor called Philip once told me at a meetup. The distinct temporality of this 'hobby' or 'leisure' activity is thus differentiated from labour, thereby suspending the regular rhythm of everyday sociality (Stromberg, 2009). Framing NFT trade as *playtime* therefore generates a designated *rhythm* that is taking place exclusively in the world of the masked, which is elusive and deceiving for all those who take part in it. The repetition of this rhythmic game of mirror across many relevant encounters, online or offline, pulsates side-by-side with the rhythm of everyday economic encounters, thus turning NFT playtime into a distinct temporal and spatial universe that is nevertheless exciting for those who dwell in it because it is never predictable (see Handelman, 2021). Playtime rhythm of collectibles, in short, continues to define NFT sociality intrinsically during negotiations on value. As Vita Peacock argues, following Lefebvre (2009) and Deleuze (1994), in the Introduction to this volume:

> Besides bodies, critical for rhythm is repetition, whether at exact intervals such as the thud of a metronome, or irregular repetitions such as seasons or tides. Like Gilles Deleuze (1994), repetition for Lefebvre is never simply replication. Though repeated, every repetitive occurrence takes place in conditions of difference, and therefore possesses the potential to reshape subsequent rhythms.

Secondly, and as a consequence, NFT sociality is playful because its ever-pulsating rhythm produces a thrill similar to that experienced in gaming. The digitality of NFTs, which, after all, are encrypted images made of pixels, turns the act of collecting them from a slow task of accumulation into a fast-moving rush to win a jackpot, as is the case with *ilinx* (whirlpool) forms of play. That is so because the rhythm of exchange relations here opens a new space of sensory and cognitive immersion that requires concentration, devotion, and risk taking, all of which are key elements in gaming (Vanolo, 2018). In fact, the aesthetics that dominate NFT sites build heavily on video game graphics, which include dark background, colourful icons, animated avatar profiles, and 'airdrops' of 'free' merchandise (such as items from an NFT series, discount codes, and entry tickets to related events). These gaming techniques structure a space in which 'trade' maintains a sense of playful unseriousness (Holloway, 2019), which is distinct from the more calculated world of cryptocurrencies trade, now already defined by some investors as 'decentralized financial investment' (DeFi).

Thirdly, at the level of daily encounters, NFT sociality is playful because it includes a high degree of role-playing, mimicry, and performance, online or offline, which inject a measure of uncertainty to most encounters in this space (Faustino et al, 2022). As the opening vignette indicates, perpetual awareness to detail, and a measure of suspicion, is built into NFT meetups, where traders meet primarily to discuss, drink, share information, and strike partnerships that could yield money in the future. To understand how this relates to play, it is important to emphasize the double nature of uncertainty. In games, a measure of uncertainty means that the result can never be known in advance (Ashtari and de Lange, 2019). If the final score of a football match was predetermined, the game would have no value. Secondly, uncertainty is anchored in the duplicity of symbols, actions, and messages. A broomstick that represents a horse during play is *simultaneously* a broomstick and a horse (Handelman, 1998). In play, as Don Handelman (1998, p 68) says, 'one thing is another, but it could be both and therefore neither'. Handelman argues that this second sense of uncertainty is endemic to any form of play, inducing doubt to the extent that players sometime wonder whether the playtime is no longer playful.[4] It is this deeper sense of uncertainty that I wish to explore in relation to play in the NFT world.

Uncertainty

While blockchains are considered 'immutable' digital environments – that is, it is difficult to hack them – swindlers can use deception, performance, and make-believe play to steal money from 'honest' traders. For example, some fraudsters have created fake NFTs that mimic genuine digital art or collectibles, selling these counterfeit NFTs to unsuspecting buyers. Phishing schemes are another preoccupation, wherein a person or organization would set up fake NFT marketplaces or websites to trick users into providing their private keys or wallet information. Once obtained, scammers can steal cryptocurrencies or NFTs from these wallets. Problems can also emerge from the fact that there is little or no legal regulation on financial activities taking place on blockchains. For example, organized groups of 'scammers' can artificially inflate the price of an NFT through coordinated buying, hyping (or 'booming'), and social media promotion. After the price has surged, they sell off their entire holdings, and convert the money into normative state-regulated currencies such as the dollar or euro, which often results in a value crash. Preoccupation with fakery, 'scamming', and fraud in NFT sociality also emerges from the fact that these tokens are traded 'on one's own responsibility', as a trader called Jonathan told me in an interview. Trading platforms are not accountable for each user's activities, and they are therefore not expected to reimburse sellers or buyers unless the platform's own account is being hacked.

A Reddit post written in mid-2022 by the pseudonymous user Reecekidd illustrates this logic. Published on the Ethereum Reddit forum and written in first-person prose, the author recounted how he fell into a series of NFT scams while trying to buy and later also mint NFTs (that is, create and connect an NFT into a blockchain). The narrative presents Reecekidd as a dumbstruck newbie blinded by the possibility of quick profiteering in the emergent Web3 ecosystem, whose lack of technical knowledge increasingly leads him to ignore warning signs, take more risks, and make more mistakes. Reecekidd writes:

> I clicked on the verify link [to join an NFT Discord community] and a login popped up. This was strange. My wallet is a Google Chrome

> plugin that should always keep me logged in. Did it time out for a security measure? I typed in my password without thinking. The plugin accepted it. But it said for additional security information, it needed my secret phrase … I went and got my secret phrase and entered it. When I entered it, nothing happened. It just said error. I entered my password and secret phrase for the second time. This is when I realized I had f***ed up. What I had entered my password and secret phrase into wasn't the official plugin. It looked the same, but it belonged to some randomer living in a shack in a different country … A better person than me would have realized they needed to be more careful. But I'm not a better person. I still wanted my NFT. I figured I had some time before the randomer would steal all my money. Like all addicts, I looked for my next hit.[5]

Reecekidd exposed in this post only some of the common schemes used by scammers to deceive and dupe unsuspecting newcomers. Readers who commented on the post generally belittled and laughed at Reecekidd, for having identified these schemes always just a moment too late, and for having continued to fall into new traps as he went along. A reader named OxPendus, for example, writes:

> You're actually just too dumb for this. And I don't mean that in a rude way. You have the self awareness to realize the mistakes you made but you feel for everything in the book and it was all driven by your desire to get rich quick. Stop and ask yourself 'is it likely that the guy who fell for multiple scams in one day without deep technical knowledge will end up striking gold and making it rich from a few pixels?' No. The answer is no. You're not that guy. I have sympathy for the pain you're in now but it's entire [sic] self inflicted due to greed. You need to accept the fundamental lesson that you are an outsider in this space – you're the sucker everyone else is making the millions from.

Other readers understand the parody in between the lines, however. Rather than reflect incidents that happened to a single person, the story seems to have wittingly used a composite personality to ridicule or accentuate a series of real-life events common in the hype of NFT trade that at the time was booming. A commenter named Psukhe, who may have realized the joke, summarizes its moral lessons as a form of advice to other newcomers:

> Great post, fear of missing out [FOMO] and the allure of easy money is strong. It causes you to panic, and there are so many scams out there. Sorry it happened to you but consider it a $300+ lesson. Your journey was probably similar to many others, people can read this post and not

> make the same mistakes. Make sure to disable DMs [Direct Messages] in new discord servers you join, there are inflated fake discord user numbers, discords mods and admins can get hacked and send out links in official channels. *Don't move so fast that you forget to take the time to double check* … Good luck out there!

NFT traders act in an environment drenched with suspicion, which is subjected to a continuous sense of uncertainty, which thus has a transformative appeal and power that lasts beyond the designated temporality of the play itself, as it constitutes a general attitude (Handelman, 2021). Partly this ongoing atmosphere of suspicion is preserved because, unlike financial transactions that go through credit card companies, blockchain-enabled transactions do not enjoy legal protections. Cryptocurrency and NFT transactions are also irreversible, so it is nearly impossible to retrieve lost or misdirected funds. In fact, as fraudsters increasingly improve their tactics, NFT collectors, creators, and sellers have increasingly also begun exercising extra caution, conducting due diligence, and identifying potential risks. As Psukhe claims in the previous extract, traders must move slowly and 'take the time to double-check' who they are interacting with, thus ultimately turning the act of monitoring into a distinctly temporal issue.

Temporal monitoring

Surveillance in the playful world of NFT traders is a serious business, which is enacted rationally to either protect or steal money. Without monitoring – both in the sense of self-control, self-discipline, and self-tracking, and in the sense of observing and measuring others in the 'space' – there can be no financial securitization. Once you are in this game, you need to know what you are showing to whom, who is an ally and who is a foe, and what types of masks or deceptive strategies swindlers might use to put their hands on your money (or money-like tokens, such as NFTs). There is a spatiality to this act of monitoring – you need to verify that things are correctly positioned in their digital space. An account out of place, a transaction going to the wrong address, and so on, can result in economic loss (see Thompson, 1967). You must therefore scan the horizon constantly for those who fake in contrite spirit, who seek direct scamming (Swartz, 2022). Monitoring under these conditions has two main manifestations.

At the technical level, experienced NFT collectors would first verify that they were investing in genuine assets. To do that, they can use designated sites where you can audit the token to determine how likely it is to be fraudulent.[6] They would typically check whether the cryptographic code that identified a token they wished to buy was registered on the Ethereum network, the main blockchain used for storing NFTs; read the comments section in different sites that scan blockchain tokens to verify their authenticity; Google-search to see if a personal page or a site of the seller can be located; check blacklists that are published by both scanning sites and exchange platforms on a regular basis; and verify that the token they are buying is registered on the main exchange platforms. One of the rules of thumb is in fact *never* to post NFTs on – or buy them from – unknown or newly created marketplaces.

Meanwhile at the level of social interaction, monitoring focuses on verifying the identity of interlocutors on common digital platforms that traders use for networking and communication. These mainly include LinkedIn, Reddit, Twitter (now called X), Telegram, Discord, and several meetup applications, which are used to organize social events offline. On Discord channels, which host most NFT self-proclaimed 'communities', moderators continuously publish warnings and actively encourage members to double-check any interaction they have with others online. Since all peers are equal in their ability to track and produce information on the blockchain, and the many relevant forums used to sustain NFT sociality online, both honest and dishonest NFT traders must monitor themselves and other users all the time. This creates a social landscape characterized by total visibility: everyone keeps watching everyone else's movements to make sure they cannot be harmful to them, on the one hand, or expose them as 'scammers' on the other. For example, a moderator in an NFT Discord community, in March 2022 published the following warning:

> We've heard one too many stories of people in the NFT community losing their assets or getting scammed. We typed up this guide to help you avoid the most common scams and keep your accounts and wallets safe.
>
> **Rule #1:** *Don't click on links from strangers.* If you need to get somewhere, try googling it or going through a project's official twitter accounts.
> **Rule #2:** *Disable Discord DMs* from server members, and *enable two factor authentication*.
> **Rule #3:** If in doubt, open a □▌HELPDESK [chat box] before you do *anything*.
>
> **Rule #1 is most important –** don't click on links or connect to sites someone has asked you to visit … *Keep an eye out for similar messages and report them!*

As in the film *Brazil* (1985), a social landscape drenched with suspicion transpires here through a continuous demand to monitor everything.[7] Business opportunities, financial security, and the sheer ability to trade or collect all emerge from the ability (and skill) to use surveillance as integral to any other social calculation. Abiding by rules of thumb meant to protect so-called 'honest' traders, thus becomes a vector of individual control designed to produce securitization and independence. For example, in a Reddit post from 2023, a user called FSmertz described a potential scammer who provoked their suspicion. They ask community members for their opinions, as they were still interested in receiving their commission in case it was a genuine buyer. The full message reads:

> Got a private message a couple of days ago on Instagram asking if I can do a painting for her. I said yes and now she is very keen to put the money into my account right away via PayPal before I have a chance to discussed [sic] more details. Her profile name is very common and is the same name as a famous American actress. She only has four post [sic], the oldest being a mouth [sic] old. I ask her if we can do a different payment method than paypal [sic] but said she can only do paypal [sic]. I've heard about paypal [sic] scams from other artist and worried this may happen to me. Am I being paranoid or should I just take the commission?'

Based on the description, all responders agree that the potential customer must have been a scammer, advising FSmertz to 'run-away', 'block', and 'delete'. One of them provides the following answer:

> Its [sic] could be a scam. I had a personal experience from Instagram a few months back. They pretended to have put the money in my account, than [sic] an email was sent that I was to refund $200 due to [use of] different currencies. My partner helped me and rang PayPal and read the email to customer service and they were excellent in determining it was [a] scam just by the 'invoice number'. *Be vigilant, your time is too valuable to waste on these nonces* [sic].

The call for vigilance, seen as a time worth investing in order to avoid wasting investors' time later on, is reiterated during physical meetups I attend in London. In another meetup organized by Laura and Jim, her co-organizer, for example, the initial welcome speech includes a direct appeal to 'those of you in the room who are after the easy money' not to promote illegitimate or fraudulent NFT products. 'You will be wasting our time, and also yours', said Laura. In an interview with Wanderlei, a Brazilian-born London-based artist who has, in recent years, been selling his art via Instagram, he likewise mentions the 'loss of time':

> I work on [both] my prints and digital pictures for weeks at a time, you know. I design them based on traditional symbols and images [from

> Brazil] and this is a lengthy process. I print them physically, take photos, and post them on my Instagram page. Because of all that investment, not just of money and material but also energy and all those weeks or even months [for production], I just don't want to take the chance that someone will scam [sic] me. I am [not] going to waste my time and eventually likely also to lose money. I don't need this.

Naturally, then, active swindlers also monitor the persons they are attempting to scam. Gus, a research interlocutor from London, shares a screenshot of a conversation on Telegram with an unknown person, using the alias Sherron T. Moore. 'Sherron' approached Gus unexpectedly, and at some stage during their conversation dropped in the word 'Ayale'. Gus quickly Googled the word and discovered that it is a Yoruba term used by West African fraudsters to test if their interlocutor might also be a 'scammer'. Gus thus replied with an 'Ayale' of his own, and the conversation swiftly moved to pidgin as the 'scammer' on the other side of the screen assumed he or she was talking with a colleague. The entire conversation between them is short, and does not include a direct reference to time. It is reasonable to assume, however, that partly the dropping of 'Ayale' sometimes at the beginning of the conversation is itself a monitoring technique aimed at 'saving' time.

In all these accounts, acts of wasting/saving time advance a double meaning. On the one hand, they are related to the labour-intensive and productivity-oriented aspects of art at large, and the creation of NFTs, in particular, which can be quantified as either loss or gain of money. On the other hand, however, 'wasting/saving time' in the context of NFT sociality is also related to the temporality of play itself, which should adhere to certain rules to be considered play at all. 'Waste of time' in that sense is the time lost for *dishonest play*, a breaking of the rules which upon its discovery retrospectively obviates the meaning of the entire playtime, turning it in fact into a form of unproductive labour on the side of the scammer. 'Saving time', then, from the point of view of those same swindlers, is thus aimed to reduce the time spent/wasted while trying to play/work (that is, to 'scam' through) a worthless game.

One of the consequences of the normalization of this temporal logic is an erosion of panoptic sensibilities, which Michel Foucault (2004, p 1) associated with the advent of 'bio-power', 'the set of mechanisms through which the basic biological features of the human species became the object of a political strategy, of a general strategy of power'. The body is increasingly becoming secondary within a regime of truth that assumes the ongoing preservation of masks all the time (Mathiesen, 1997). The game of surveillance that ensues within such a regime, which in the case of NFT sociality is enacted as part of the wider playtime of trading and collecting, abolishes the importance of corporeality, as it shifts attention from the ontological, the material, and the authentic, to the graphical, the ethereal, and the performed. The temporal implications of this transformation, as I now turn to explicate, are confining as much as they may be regarded liberating, at least as this relates to the tension between experimentalism and securitization in the unregulated space of crypto-asset trading.

Analysis

David Lyon (1994; 2007) uses the term 'post-panoptic surveillance' to describe a diffusion of power relations in the deployment of monitoring. As opposed to the panoptic model of surveillance (Foucault, 1991), which is spatially confined and which assumes an unbridgeable yet clearly observed distance between those who monitor and the subjects of monitoring, post-panoptic surveillance is spatially dispersed. It assumes concealed forms of monitoring as much as it uses other forms openly (for example, CCTV), to deter and restrict potential deviance in the public sphere. Post-panoptic surveillance turns the top-down exploratory gaze of the panopticon into a heterogeneous, space-level, all-encompassing inspection, which can be employed in any direction and towards any 'target' (Albrechtslund and Lauritsen, 2013). The sociality around NFT trade is 'post-panoptic' because it makes ongoing monitoring a *necessity*. In a reality marked by playful performances, masking, pretensions, uncertainty, and suspicion, constant monitoring simply becomes the natural thing to do and the most important survival strategy, both at the technical level and as a skill required to navigate social relations (See Staples, 2013 [2000]).

Post-panoptic surveillance technologies thereby perpetuate the spell of Prediction (with an uppercase P) as a preferred method for designing anticipated futures (Hong, 2022; compare Kitchin, 2014). The establishment of post-panopticism on a large scale helps distribute the idea that Prediction is positive and necessary. In the case of NFTs, as I demonstrated earlier, Prediction relates to anticipating and thwarting 'scams' as integral to regular encounters. However, this same process also works to validate facts retrospectively by seeking to concretely identify objects such as names (for example, scammers) or events (for example, a phishing attack in a forum). In NFT sociality, retrospective identification of a scam can be disheartening, as some of the responses to Reecekidd's post quoted previously make clear. This duality reveals a normative dimension that organizes NFT trade – the requirement to identify a potential trap translates into the promulgation of suspicion and the reification of certain values, especially regarding the binary distinction between 'honest' and 'fraudulent' actors. Time dedicated 'now' to risk aversion – manifesting in the disposition to 'double-check' everything – becomes a murky liminal territory between legitimate and illegitimate datafication of play-forms (van Dijck, 2014), which are retrospectively defined as a 'wasted time' in case a fraud has indeed been detected.

Hong's analysis exposes a double temporality that is intrinsic to post-panoptic realities: on the one hand, surveillance works progressively to justify the truth of Prediction, but on the other hand, it works recessively to justify hegemonic moral values (of which Prediction is an essential part; Hong, 2022). Prediction in that sense, paradoxically, extends a concrete, grounded vision of the present, which often relies on abstract notions of order and control (Frois, 2013; Kitchin, 2014) and on concrete agents that wield the power to sanction (Zuboff, 2019). The operative and pre-emptive temporal logics that drive surveillance practices in NFT sociality can thus be seen to universalize themselves, becoming ubiquitous as they are applied, and thus also extending the real or imaginary threat conditions for which they were invented in the first place. Surveillance as a tool aimed at protecting the self, consequently drives the perfection and innovation of better monitoring technologies, which deepen and totalize the present order even further into the future (Hong, 2022).

The temporality of post-panoptic monitoring in the world of NFT collectors thereby generates a game of hide-and-seek, in which power itself is constantly disguised and revealed unexpectedly (Lyon, 2018). Arising from within the ranks as it sinks back into anonymity, the power to swindle and the power to defend oneself against swindling is embedded in the ability to track and observe others almost all the time (Maras and Wandt, 2019). Those who appropriate and operationalize better monitoring and tracking techniques gain a significant advantage, a fleeting dominance over nearly arbitrary others. Sometimes this comes at the expense of others, as with outright 'scamming', and sometimes it is a mere fencing technique. When NFT traders normalize acts of monitoring and surveillance as boundary-making techniques that securitize their funds in the present for a sense of a more certain future, they effectively mimic the exploratory gaze employed by hackers and scammers, a gaze they are otherwise trying to block or evade. This scrutinizing gaze, allegedly characterizing only those malicious actors seeking a scamming opportunity, here emerges almost by definition as an ethical common demeanour in a sociality defined by play, masking, and accelerated movement. The very act of masking, which is endemic to both play and barter, becomes essential for NFT playtime activities at large.

An empirical game of hide-and-seek in this context opens possibilities to think about self-expression in situations of algorithmic visibility (O'Neil, 2016). A traditional *panoptic* approach assumes that self-expression under a scrutinizing gaze produces docility and a desire to satisfy the observer. Resistance in this situation can only be practised in dead spots, where observers cannot exercise their power. Self-expression in *post-panoptic* realities has contrarily been celebrated as inherently resistant and even liberating because it appropriates surveillance to the goals and interests of the observed (Albrechtslund, 2008). Here, technologies of visualization and representation (such as chats) become emancipatory tools for genuine personalized desires, on the one hand, or means to manipulate and commercialize an audience voyeurism on the other (Staples, 2013 [2000]). But what do we do with self-expression in and around blockchain-based sociality, wherein every single peer is simultaneously the observer and the observed? What do we do with power and resistance in a 'networked' environment composed of a multiplicity of tightly interconnected peers, who always watch one another while being watched by everyone else?

Conclusion

Rather than social persons in the sociological sense of the term, which always includes bodies as the ultimate space of political contestation, a temporal logic of surveillance in the world of NFT collectors contributes to the emergence of purified perspectives, from which people can explore or even scrutinize others. I here follow the late John Perry Barlow, a pioneer of techno-utopianism in cyberspace and a renowned American poet. In 1990, Barlow published an account of his first experience with a virtual reality machine in which he claims that he was 'reduced to a point of view' (Turner, 2006, p 165). Amazed by the lack of corporeality of the experience, Barlow described how everything suddenly became possible within a three-dimensional cyberspace. Barlow claimed that the adoption of this gaze, a reductionism into a position of a total observer, also entailed epistemological transformations. Operating freely as a 'point of view' in the context of NFT monitoring, ultimately demands not only technical knowledge (that is, how to verify the authenticity of tokens), but also: (1) the embodiment of a new set of moral codes that distinguish right from wrong (that is, what kinds of half-truths are acceptable and which ones would be considered deception); and (2) the implementation of these moral codes through concrete acts of ethical decision-making (that is, when it is okay to 'DM' [direct message] someone, proper ways to speak with others online and offline about NFT trade, and so on).

Playtime, as it is empirically grounded in acts of surveillance, goes beyond NFT trade or even the involvement in other, more risky, blockchain assets. Among many contemporary examples, the gamification of cityscapes seems to be especially relevant for the intensification of a post-panoptic temporal dynamic of surveillance, that builds distinct playtimes and play-spaces wherein all interactions are closely monitored (Ruffino, 2014; Maras and Wandt, 2019). 'In its essence', argues Alberto Vanolo:

> gamification concerns the mobilisation and implementation of ludic elements – or, better to say, videoludic elements – in order to manage

> 'serious' and 'real' issues … By introducing game mechanics such as rankings, scores, badges, levels, rewards and virtual currencies in apps and websites originally distant from gaming cultures, software designers and policy makers aim at stimulating public engagement and virtuous social behaviours. (Vanolo, 2018, p 320)

Gamification apps in urban spaces are often designed to increase awareness to sustainability issues by incentivizing the users to engage in fun activities and play scenarios, thereby ultimately impacting and modifying behaviours (Kitchin, 2014). In that sense they also sometimes work to coerce, tacitly, or even enforce, certain types of behaviours in public. The same temporal logic undergirds NFT monitoring, wherein 'awareness' is integrated into mundane actions to predict present as well as future threats. I hope this chapter will encourage colleagues to conduct more research on this process.

Notes

[1] Mining is an ongoing competition between computers to decipher a complicated cryptographic code, which conceals a set number of digital coins. The first computer to decrypt the code 'extracts' these coins from its digital storage and gets to keep them. They are then traded online on designated platforms using other types of currency, either digital or state-controlled fiat money.

[2] Web3 refers to emergent decentralized internet infrastructure, which, unlike Web2 applications, enables content creators to own and commercialize their data using blockchains and NFT-like digital signatures. Metaverse is a general category for the use of virtual reality (VR) headsets to engage in virtual environments in a more immersive way than is usually enacted today. Whereas VR glasses are now mainly used for gaming, metaverse activities can include many other mundane activities, such as professional meetings in workplaces and online concerts.

[3] Caillois distinguishes between structured games, which, following Huizinga (1970 [1939]), he calls *ludus*, and unstructured and spontaneous play, which he calls *paidia*. The four types of play occur in each of these modes.

[4] On the one hand, duplicity in play affords flight of the imagination, but on the other hand, it can cause confusion and breakdown that would spill over into mundane reality. This is so, as Gregory Bateson (1972) argued, because any playful action *could* be interpreted as if it was entirely serious. For example, I once watched a performance of a clown that included controlled, yet deliberately abusive interaction with the audience. About halfway through the stint, one of the volunteers, who was drunk, suddenly stood up, grabbed a half-empty beer bottle, and broke it on the clown's head. He then screamed that he would not tolerate such abuse and ran away before security could reach him. This radical reaction resulted from the uncanny feeling that the clown's words *could* have been serious, rather than playful.

[5] https://www.reddit.com/r/ethereum/comments/tz7p9w/i_fell_for_every_nft_scam_in_10_minutes/?rdt=57683 (Accessed: 26 February 2025).

[6] Such as www.dappradar.com (DAPP = Decentralized Apps) (Accessed: 26 February 2025).

[7] Gilliam's dystopic parody playfully ridiculed some of the darker fantasies of the genre by using different signs that were embedded in the set. For example, a poster that was hung on the office wall of one of the protagonists read: 'Don't suspect a friend, report him'. Another poster, however, read: 'Suspicion breeds confidence'.

References

Albrechtslund, A. (2008) 'Online Social Networking as Participatory Surveillance', *First Monday*, 13(3): 1–10.

Albrechtslund, A. and Lauritsen, P. (2013) 'Spaces of Everyday Surveillance: Unfolding an Analytical Concept of Participation', *Geoforum*, 49: 310–16.

Antonopoulos, M.A. (2016) *Mastering Bitcoin*. Sebastopol: O'Reilly Media.

Ashtari, D. and de Lange, M. (2019) 'Playful Civic Skills: A Transdisciplinary Approach to Analyse Participatory Civic Games', *Cities*, 89: 70–9.

Bateson, G. (2000) [1972]). *Steps to an Ecology of Mind*. Chicago, IL: University of Chicago Press.

Borch, C. (2007) 'Crowds and Economic Life: Bringing an Old Figure Back In', *Economy and Society*, 36(4): 549–73.

Caillois, R. (2001 [1961]) *Man, Play, and Games*. Urbana, IL: University of Illinois Press.

Deleuze, G. (1994) *Difference and Repetition*. London: Athlone Press.

Derrick, J. (2021) 'Crypto security breaches are up 850% in the last decade', Invezz.com. Available from: https://invezz.com/news/2021/12/16/cryptocurrency-security-breaches/ (Accessed: 27 January 2025).

Faustino, S., Faria, I., and Marques, R. (2022) 'The Myths and Legends of King Satoshi and the Knights of Blockchain', *Journal of Cultural Economy*, 15(1): 67–80.

Foucault, M. (1991) *History of Sexuality Vol. 1: An Introduction*. New York: Vintage Press.

Foucault, M. (2004) *Security, Territory, Population: Lectures at the Collège de France, 1977–78*. Edited by M. Senellart. Translated by G. Burchell. London: Palgrave MacMillan.

Frois, C. (2013) *Peripheral Vision: Politics, Technology, and Surveillance*. New York and Oxford: Berghahn Books.

Handelman, D. (1998) *Models and Mirrors*. Oxford: Oxford University Press.

Handelman, D. (2021) *Mobius Anthropology: Essays on the Forming of Form*. Edited by M. Shapiro and F. Jackie. New York and Oxford: Berghahn.

Holloway, D. (2019) 'Surveillance Capitalism and Children's Data: The Internet of Toys and Things for Children', *Media International Australia*, 170(1): 27–36.

Hong, S. (2022) 'Predictions Without Futures', *History and Theory*, 61(3): 371–90.

Huizinga, J. (1970 [1939]) *Homo Ludens: A Study of the Play Element in Culture*. London: Maurice Temple Smith Ltd.

Kitchin, R. (2014) 'The Real-Time City: Big Data and Smart Urbanism', *GeoJournal*, 79(1): 1–14.

Lefebvre, H. (2009) *Rhythmanalysis: Space, Time and Everyday Life*. Translated by S. Elden and G. Moore. London and New York: Continuum.

Lyon, D. (1994) *The Electronic Eye: The Rise of Surveillance Society*. Cambridge: Polity Press.

Lyon, D. (2007) *Surveillance Studies: An Overview*. Cambridge: Polity Press.

Lyon, D. (2018) *Surveillance, Power, and Everyday Life*. Oxford: Oxford University Press.

Maras, M.H. and Wandt, A.S. (2019) 'Enabling Mass Surveillance: Data Aggregation in the Age of Big Data and the Internet of Things', *Journal of Cyber Policy*, 4(2): 160–77.

Mathiesen, T. (1997) 'The Viewer Society: Michel Foucault's Panopticon Revisited', *Theoretical Criminology*, 1(2): 215–34.

Nakamoto, S. (2008) Bitcoin: A Peer-to- Peer Electronic Cash System. Open Access Online. Available from: https://bitcoin.org/bitcoin.pdf (Accessed: October 2023).

O'Neil, C. (2016) *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown.

Ruffino, P. (2014) 'From Engagement to Life, or: How to Do Things With Gamification?', in M. Fuchs, S. Fizek, P. Ruffino, and N. Schrape (eds) *Rethinking Gamification*. Lüneburg: Meson, pp 47–68.

Smith, C.W. (1999) *Success and Survival on Wall Market*. Oxford: Rowman & Littlefield.

Staples, W.G. (2013 [2000]) *Everyday Surveillance: Vigilance and Visibility in Postmodern Life*. Oxford: Rowman & Littlefield.

Stromberg, P.G. (2009) *Caught in Play: How Entertainment Works on You*. Stanford, CA: Stanford University Press.

Swartz, L. (2022) 'Theorizing the 2017 Blockchain Ico Bubble as a Network Scam', *New Media & Society*, 24(7): 1695–713.

Thompson, E.P. (1967) 'Time, Work-Discipline, and Industrial Capitalism', *Past & Present*, 38(1): 56–97.

Turner, F. (2006) *From Counterculture to Cyberculture: Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism*. Chicago, IL: University of Chicago Press.

van Dijck, J. (2014) 'Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology', *Surveillance & Society*, 12(2): 197–208.

Vanolo, A. (2018) 'Cities and the Politics of Gamification', *Cities*, 74: 320–26.

Zimmer, Z. (2017) 'Bitcoin and Potosí Silver: Historical Perspectives on Cryptocurrency', *Technology and Culture*, 58(2): 307–34.

Zuboff, S. (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs.