Between Cypherpunks and Commons. Navigating Blockchain's ideology of social change

Paula Ungureanu[3]

As new technologies afford to do things that were previously thought to be beyond the grasp of mankind (e.g., flying, space travel, extensive manipulations of nature, complicated medical interventions) they acquire the select status of objects that transcend the everyday and may even become objects of intense emotions such as wonderment and worship (Pärna, 2010). Historian and technology critic David Noble describes technologies to which great hope is pinned and which are typically hailed as the means of overcoming the shortcomings of the human condition as "technologies of transcendence" (Noble, 1998). In their early days, the steam engine, the railroad and the telegraph were heralded as instruments that would conquer time and space, alleviate poverty, and elevate wellbeing (Alexander, 2003; Standage, 2005). The commoditization of personal computers in the mid-1980s, the introduction of Internet and the rise of the knowledge economy a decennium later, released new waves of such faith (Nisbet, 2017; Pärna, 2010). Today, emergent digital technologies—including artificial intelligence, virtual reality, and blockchain—command a similar fervor and collective expectation for radical social change (Bailey, Faraj, Hinds, Leonardi, & von Krogh, 2022; Benbya, Davenport, & Pachidi, 2020; Faraj, Pachidi, & Sayegh, 2018).

Blockchain, in particular, is hailed as one of the most powerful of these new technologies, often compared to the Internet in its potential to reshape economic, political, and social structures (Catalini & Gans, 2020; Davidson, De Filippi, & Potts, 2018; Felin & Lakhani, 2018). Its emergent applications have generated visions of a new world, powered by decentralized, peer-to-peer trust systems that bypass traditional intermediaries such as banks, states or private gatekeepers (Jacobetty & Orton-Johnson, 2022). By emphasizing cryptographic security, individual freedom, and a movement away from centralized authority, blockchain technology presents itself as a vehicle for profound systemic change (Catalini & Gans, 2020; Davidson et al., 2018; Notheisen, Hawlitschek, & Weinhardt, 2017).

However, blockchain is not an invention that emerged from pure technical ingenuity alone; it draws heavily on ideologies that have long questioned centralized power structures. While Satoshi Nakamoto's (2008) white paper introduced Bitcoin and its associated blockchain as fundamentally decentralizing technologies, his work built upon decades of ideological exploration, including the cypherpunk's rage against governmental surveillance, the libertarian ideals of individual autonomy, and even the early notions of an information commons where knowledge and code should be open and collectively managed.

As new technologies often attract utopian visions of social change, the question arises: how do these ideologies shape our expectations? While blockchain technology is often framed as a solution to the failures of institutions and social systems, it is essential to inquire how its embedded ideologies influence its transformation into a utopian, yet often polarizing, force within contemporary society. This essay seeks to explore the relationship between blockchain technology ideologies—specifically cyberlibertarian thought—and the concept of the commons. It simulates reflection on what exactly blockchain technology promises—and how these promises relate to historical and ongoing debates about the commons, shared resources, individual agency and collective governance.

Blockchain's cyberlibertarian ideology: from cypherpunks to crypto anarchism and beyond

Although blockchain entered the public arena in 2008 with Bitcoin, its ideological roots extend back to the late 1980s and the early 1990s, when a community of cryptography enthusiasts—known as cypherpunks—began exploring the potential of encryption for social and political change. These early advocates, largely drawn from mathematics, computer science, and cryptography, held that robust encryption was not merely a technical tool but a moral imperative to preserve individual freedom (Swartz, 2018). The movement was a reaction to growing concerns about surveillance and state control over digital communications and saw in cryptography an ideal tool to protect privacy and enable secure, anonymous digital interaction. Nick Szabo, a cryptographer and early blockchain theorist, explored how decentralized, self-executing agreements could enable a stateless, cyber-anarchist economy. Through his close relationship with the cryptographic community (sometimes called "crypto banks" or "cipher banks") and its informal leader Timothy C. May, the author of the famous "Crypto Anarchist Manifesto" (May, 1992), allowed Nick Szabo to lay the grounds for the original concept of crypto economy (Judmayer, Stifter, Krombholz, & Weippl, 2017). Szabo is credited for being the inventor of smart contracts—self-executing contracts written into code—which later became a core feature of blockchain technology(Szabo, 1996), and was the proponent of Bit Gold (Szabo, 2005), a decentralized digital currency that used computation to generate cryptographic puzzle solutions, much like Nakamoto's 2008 proposal of Bitcoin.

[3] Department of Sciences and Methods of Engineering (DISMI). University of Modena and Reggio Emilia. paula.ungureanu@unimore.it

A closely related movement was that of crypto anarchism, a political philosophy that, in its idealized form, recognizes no laws except those that can be described by math and enforced by code. Crypto anarchism takes cypherpunk principles a step further, advocating for the complete erosion of state authority in digital spaces. While cypherpunks focused on protecting privacy, crypto-anarchists sought to actively undermine state power by creating an alternative, stateless digital economy(Beltramini, 2021). As Duncan Frissell put it in a post to the Cypherpunk email list in 1996, they positioned blockchain in opposition to the current capitalist system, such that *"future market societies [would] no longer be in the hands of "The Authorities" but rather in the hands of those trading on the market; i.e. everyone on earth"* (Swartz, 2018: 267). Other key exponents of crypto-anarchism such as Timothy May (1992), John Perry Barlow (1996) and Julian Assange (2012) further championed these ideals envisioning a world where strong cryptography could dismantle state surveillance and coercion, allowing individuals to interact freely without government oversight. The cyber anarchists coined the term 'cyberspace' which they viewed as a realm of radical freedom, self-governance, and resistance to state and corporate control. While their perspectives varied, they shared a belief that digital technologies—particularly encryption, decentralized networks, and open-source systems—could be leveraged to create a borderless, autonomous space beyond traditional political and economic structures. In "A Declaration of the Independence of Cyberspace", Barlow (1996) famously declared cyberspace as independent from nation-states. He envisioned the internet as a new, self-regulating domain where individuals could interact without interference from governments that did not "possess sovereignty" over this digital world. For Barlow, cyberspace was a utopian space of pure speech and free association, where traditional hierarchies and laws were irrelevant, while for Assange, cyberspace was a tool to expose corruption and dismantle secrecy-based power structures. WikiLeaks embodied this belief: by leveraging cyberspace, it forced institutions into involuntary openness, weakening their control over information.

With the devastating surge of the 2008 Financial Crisis and the systemic loss of trust in governments, regulatory authorities and financial institutions, these ideas found their way into the mainstream, as Satoshi Nakamoto's cryptocurrency project, Bitcoin, gained massive recognition as the most famous blockchain application and one of the most radical revolutions after the world wide web (Davidson et al., 2018). Satoshi Nakamoto's (2008) Bitcoin whitepaper references many of the same cryptographic and decentralization principles that Szabo explored with Bit Gold, and that cyber-anarchists associated to the cyberspace. Since its unveiling, Bitcoin has intrigued with its ability to support currency on a global scale and coordinate exchanges in large communities of users without centralized control or infrastructure thanks to the decentralized and immutable technology called blockchain (Judmayer et al., 2017).

In synthesis, blockchain is a decentralized digital ledger that securely records transactions across a network of computers, ensuring data is transparent and tamper-proof. Each transaction is grouped into a "block," which is then linked to the previous one, forming a "chain" of blocks, hence the name "blockchain". This decentralized structure means that no single entity controls the data, and each participant in the network possess a copy of the entire blockchain. When a transaction occurs, it is validated by this diverse network using a consensus mechanism, and cryptographically secured and added to the chain, making it immutable and visible to all network participants (Beck, Stenum Czepluch, Lollike, & Malone, 2016; Buterin, 2014; Glaser, 2017; Nakamoto, 2008; Wood, 2014).

Blockchain technology promises to revolutionize the trust processes needed in all types of human exchanges, from physical goods to rights and information, thanks to its unique socio-technical affordances (Davidson et al., 2018; De Filippi, Mannan, & Reijers, 2020; Felin & Lakhani, 2018). Decentralization, at the heart of blockchain, refers to the distribution of control, authority, or decision-making across multiple nodes or participants, rather than relying on a single central authority (Glaser, 2017; Nakamoto, 2008; Notheisen et al., 2017). For instance, Bitcoin's decentralized network allows users to send and receive payments without relying on banks or other intermediaries, democratizing financial transactions and eliminating intermediary trust (Nakamoto, 2008). Smart contracts are another innovative aspect (Buterin, 2014). Platforms like Compound use smart contracts for automated lending and borrowing (Saengchote, 2023), while IBM's Food Trust platform uses them to track and verify food products, enhancing supply chain transparency and accountability from farm to fork (Casino, Dasaklis, & Patsakis, 2019; Kawaguchi, 2019). Blockchain's transparency feature ensures all transactions are publicly recorded and verifiable, fostering accountability while cryptographic techniques secure data and transactions, protecting against unauthorized access (Pilkington, 2016).

Given the affordances above, I refer to this ideology as "cyber-libertarianism" a broad term to describe both cypherpunks' and crypto-anarchists' shared a belief in the value of technology in maximizing individual freedom and minimizing government control. While originally

closely related to cryptocurrency applications, since 2016 the uses of blockchain have significantly expanded beyond cryptocurrencies and are rapidly evolving across multiple fields, mainly due to the introduction of smart contracts. Since smart contracts automate the execution of an agreement so that all participants can be immediately certain of the outcome, without the need to know, trust, coordinate with each other or rely on intermediaries, they open up the possibility of blockchain revolutions in a wide range of sectors (Davidson et al., 2018; Felin & Lakhani, 2018). Within the trend of high volatility and exponential growth of the last years, a particular attention in the venture landscape has been given to blockchain solutions which aim at solving some of the world's toughest challenges, from poverty and access to healthcare and education, to fair and sustainable consumption, all the way to climate change (Kewell, Adams, & Parry, 2017; Ungureanu & Cochis, 2023). In line with the crypto-libertarian foundations, using blockchain for good includes as many as banking the unbanked, providing alternative models of consumption, enhancing environmental sustainable practices, democratizing peer-to-peer exchanges of goods and services, peer-to-peer microfinancing solutions and new models of humanitarian aid (Ungureanu & Cochis, 2023).

It is also noteworthy that cyber-libertarianism is deeply embedded in other technology-centered ideology. Andrew Shapiro (1999) and Pärna (2010) discussed the long-standing myth of technology as a liberator, highlighting collective beliefs of the internet's quasi-magical power to overturn millennial dynamics of power and control, enabling individuals to transcend traditional constraints of gender, race, and class and thus giving them the opportunity to realize their true potential without inhibitions. A similar narrative emerges in "Cyberspace and the American Dream" (Dyson, 1996), which likens the Internet to a new frontier—a digital Wild West free from hierarchical constraints. Rooted in the American ethos of self-determination, this perspective frames cyberspace as a domain of unregulated enterprise and individual empowerment, heralding the decline of centralized bureaucracies in favor of decentralized, personalized governance.

Blockchain ideology in between cyberlibertarianism and commons

As these examples suggest, in place of the static perfection of a utopia, crypto libertarianism envisions an "extropia", an open, evolving society allowing individuals and voluntary groupings to form the institutions and social forms they prefer (Damour & Damour, 2024). I here suggest that this ideology draws close to a commons' perspective, while also including some revolutionizing principles and some contradictions.

While blockchain ideology is deeply rooted in the quest for individual autonomy and the decentralization of power, the concept of the commons offers an alternative vision that emphasizes shared resources and collective management. The commons perspective is grounded in the idea that certain resources—such as the environment, knowledge, and digital infrastructures—should be managed collectively by communities rather than privatized or controlled by state entities. This perspective upholds values like egalitarianism, community participation, and stewardship, contending that resource management is most effective when it is democratically governed and equitably distributed (Benkler & Nissenbaum, 2006; Gardner, Ostrom, & Walker, 1990; Ostrom, 1990).

Despite these differences, both blockchain ideology and the commons share a set of commonalities. While blockchain ideology is deeply rooted in the quest for individual autonomy and the decentralization of power, it also draws inspiration from earlier visions of the information commons. Early cypherpunk writings—such as those found in the Cypherpunk Manifesto—emphasized that information should be freely available and collectively managed, free from the control of centralized institutions. The following text written by mathematician and computer programmer Eric Hughes (1993) in the Cypherpunk Manifesto exemplifies the new idea of algorithmic expertise as a collective and decentralized means of social liberation empowered by information technology:

"Information does not just want to be free, it longs to be free. Information expands to fill the available storage space. Information is Rumor's younger, stronger cousin; Information is fleeter of foot, has more eyes, knows more, and understands less than Rumor. Cypherpunks write code. We know that someone has to write software to defend privacy, and since we can't get privacy unless we all do, we're going to write it. We publish our code so that our fellow Cypherpunks may practice and play with it. Our code is free for all to use, worldwide. We don't much care if you don't approve of the software we write. We know that software can't be destroyed and that a widely dispersed system can't be shut down."

As exemplified by Hughes' (1993) Cypherpunk Manifesto, cyber libertarianism, which heralds a world of minimal state intervention and maximal individual freedom, is not entirely opposed to the commons but rather reinterprets its principles through a technological lens. Blockchain technology, with its decentralized, trustless, and secure infrastructure, embodies this hybrid vision by enabling

both individual empowerment and the creation of shared, resilient networks.

In addition, cyber libertarianism and commons also share a critical stance toward centralized power and monopolistic control. As explained above, blockchain ideology disrupts established hierarchies by leveraging decentralized technologies and cryptographic trust to enable direct, peer-to-peer interactions that remove traditional intermediaries. This approach tends to favor market-oriented mechanisms aimed at empowering individuals and fostering self-sovereignty. By contrast, the commons framework emphasizes participatory governance and collective ownership, championing cooperative management, mutual aid, and social equity. Thus, while blockchain projects often pursue disruptive, technocratic strategies to reconfigure power structures, commons-based initiatives advocate for deliberative processes and community stewardship, highlighting a fundamental tension—and potential synergy—between individual empowerment and collective needs.

It is also noteworthy that blockchain proponents advocate for disrupting established financial and political systems by leveraging code as a form of governance, while commons theorists emphasize the organic evolution of communal norms and social practices, viewing shared stewardship as essential to sustainable resource management (Ostrom, 1990). This divergence highlights a tension between technocratic approaches to decentralization and the more democratic, deliberative models championed by the commons. Yet it is precisely this tension—and the potential for synergy—that offers a rich avenue for inquiry about their interplay: How might the cryptographic mechanisms of blockchain be reconciled with, or even integrated into, commons-based models of governance and resource management?

From utopia to dystopia, and the 'cyber-space' in between: Trust, crises, and the evolution of blockchain communities

Although cyber-libertarian ideals promote decentralization, blockchain communities often face crises that reveal its limitations, pushing them to confront the need for collective governance—a key concern of the commons. The vulnerabilities of blockchains such as selfish behavior, speculation, scams and frauds, hacker attacks, manipulation, and illegal trafficking, have been shown to have enormous costs in terms of social trust, slowing down blockchain's path to wide-scale adoption (Hawlitschek, Notheisen, & Teubner, 2018; Kietzmann & Archer-Brown, 2019). These tensions become particularly evident in moments of failure, where ideological commitments to immutability and self-regulation collide with the pragmatic need for intervention and shared responsibility.

A case in point is the 2016 DAO hack in the Ethereum ecosystem, the second largest ecosystem after Bitcoin, and one of the most vibrant blockchain communities (Mehar et al., 2019). Designed as a decentralized venture capital fund governed entirely by smart contracts, The DAO embodied the cyber-libertarian dream of code-based, trustless cooperation. However, when an exploit allowed an attacker to drain millions in Ethereum, the community faced an existential dilemma: adhere to the principle of immutability and accept the loss or intervene on the blockchain network to reverse the damage. In response to the generalized crisis that the incident had produced, some influential members of the community proposed to alter the Ethereum blockchain state by implementing a fork which would have nullified the hack by reversing the system to a moment before the hack (Shin, 2022). Those who supported the interventionist solution, known as 'pro-forkers,' clashed with 'no-forkers,' who opposed it. No-forkers viewed reversing the blockchain to undo an event as a breach of blockchain's immutability and a sign of vulnerability to centralization. Despite heated debates, the Ethereum community implemented a hard fork to reverse the attack. This resulted in a split, with pro-forkers upgrading the code and no-forkers sticking to the original protocol, forming an alternative ecosystem (Ungureanu, 2025). This event illustrates how, during crises, community members might prioritize immediate interests over the principles of blockchain potentially undermining the identity and cohesion of peer-to-peer communities, which are essential in both commons and the cyberlibertarian ideologies. It is thus interesting to notice how trust in blockchain idelogy can lead to community conflicts and changes to commons.

Beyond high-profile crises, everyday vulnerabilities—scams, speculative bubbles, and governance failures—continue to challenge the cyber-libertarian vision of blockchain as a self-regulating system. While libertarian-driven projects tend to resist external oversight, commons-based approaches emphasize collective stewardship, asserting that trust arises not only from cryptography but also from social cooperation. Recurrent phishing attacks at blockchains, for example, raise the question of accountability: should responsibility lie entirely with individuals, as cyber-libertarianism suggests, or should communities develop shared protective measures, as commons governance would propose?

In sum, the DAO hack serves as a striking illustration of the tensions between cyber-libertarian ideals and the practical challenges of maintaining decentralized systems. Cyber-libertarianism champions radical autonomy, trust

in code over institutions, and minimal interference, envisioning blockchain as a self-regulating ecosystem free from external control. Commons-based perspectives, in contrast, emphasize collective governance, mutual responsibility, and participatory decision-making. These conflicts reveal blockchain's dual nature, as both a vehicle for radical individualism and a 'cybersite' of emergent communal practices. While cyber-libertarians seek to minimize institutional control in favor of market-driven, self-organized systems, commons perspectives emphasize participatory governance and mutual accountability. When crises arise—whether through hacking, scams, or governance failures—these two ideological positions come into direct conflict, revealing the paradox of decentralization: the very mechanisms designed to eliminate centralized authority can, under pressure, recreate it in new forms. The evolution of blockchain communities, then, is shaped by this ongoing negotiation —between the desire for autonomy and the necessity of collective resilience. Whether blockchain ultimately fulfills its transformative potential depends on its ability to reconcile these competing logics rather than succumb to their contradictions.

This cycle—between utopian visions of self-regulation and dystopian fears of centralization—suggests that blockchain's ideological identity is not fixed but continuously reshaped by the pressures of governance and trust. Whether blockchain ultimately reinforces cyber-libertarian individualism or evolves into a model of decentralized commons will depend on how communities navigate these recurring tensions. This essay argued that understanding blockchain's potential for social change requires examining both its ideological foundations and its ability to foster new forms of collective action. A promising path is the study of the ritualized enactment of these ideologies, where new technologies do not merely reflect but actively shape social realities that are still taking form.

Funding Statement: This work has been funded within "Trust Machines for TrustlessNess (TruMaN): The Impact of Distributed Trust on the Configuration of Blockchain Ecosystems COD. PROGETTO 2022F5CLN2 - CUP E53D23006250006 - PIANO NAZIONALE DI RIPRESA E RESILIENZA (PNRR) – Missione 4 – Componente C2. Dalla Ricerca all'Impresa -Investimento 1.1 Fondo per il Programma Nazionale della Ricerca (PNR) e Progetti di Ricerca di Rilevante Interesse Nazionale (PRIN)", finanziato dall'Unione europea – NextGenerationEU - rif. D.D. N. n. 104 del 02/02/2022".

References

Alexander, J. C. 2003. The meanings of social life: A cultural sociology: Oxford University Press, USA.

Bailey, D. E., Faraj, S., Hinds, P. J., Leonardi, P. M., & von Krogh, G. 2022. We are all theorists of technology now: A relational perspective on emerging technology and organizing. *Organization Science*, 33(1): 1-18.

Barlow, J. P. 1996. Thinking locally, acting globally. *Time*, 147(3): 76-76.

Beck, R., Stenum Czepluch, J., Lollike, N., & Malone, S. 2016. Blockchain–the gateway to trust-free cryptographic transactions.

Beltramini, E. 2021. Against technocratic authoritarianism. A short intellectual history of the cypherpunk movement. *Internet Histories*, 5(2): 101-118.

Benbya, H., Davenport, T. H., & Pachidi, S. 2020. Artificial intelligence in organizations: Current state and future opportunities. *MIS Quarterly Executive*, 19(4).

Benkler, Y., & Nissenbaum, H. 2006. Commons-based peer production and virtue. *Journal of political philosophy*, 14(4).

Buterin, V. 2014. A next-generation smart contract and decentralized application platform. *white paper*, 3(37): 2-1.

Casino, F., Dasaklis, T. K., & Patsakis, C. 2019. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and informatics*, 36: 55-81.

Catalini, C., & Gans, J. S. 2020. Some simple economics of the blockchain. *Communications of the ACM*, 63(7): 80-90.

Damour, F., & Damour, F. 2024. The First Blockchain: Bitcoin, Entropy, Religion. *Zygon: Journal of Religion and Science*, 59(1).

Davidson, S., De Filippi, P., & Potts, J. 2018. Blockchains and the economic institutions of capitalism. *Journal of Institutional Economics*, 14(4): 639-658.

De Filippi, P., Mannan, M., & Reijers, W. 2020. Blockchain as a confidence machine: The problem of trust & challenges of governance. *Technology in Society*, 62: 101284.

Dreyfus, S., & Assange, J. 2012. Underground: tales of hacking, madness and obsession on the electronic frontier: Canongate Books.

Dyson, E. 1996. Cyberspace and the American Dream: A Magna Carta for the Knowledge Age (Release 1.2, August 22, 1994). *The information society*, 12(3): 295-308.

Faraj, S., Pachidi, S., & Sayegh, K. 2018. Working and organizing in the age of the learning algorithm. *Information and Organization*, 28(1): 62-70.

Felin, T., & Lakhani, K. 2018. What problems will you solve with blockchain?: MIT Sloan Management Review.

Gardner, R., Ostrom, E., & Walker, J. M. 1990. The nature of common-pool resource problems. *Rationality and society*, 2(3): 335-358.

Glaser, F. 2017. Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis.

Hawlitschek, F., Notheisen, B., & Teubner, T. 2018. The limits of trust-free systems: A literature review on blockchain technology and trust in the sharing economy. *Electronic commerce research and applications*, 29: 50-63.

Hughes, E. 1993. A cypherpunk's manifesto. *retrieved at hughes@soda.berkeley.edu*.

Jacobetty, P., & Orton-Johnson, K. 2022. Blockchain Imaginaries and Their Metaphors: Organising Principles in Decentralised Digital Technologies. *Social Epistemology*: 1-14.

Judmayer, A., Stifter, N., Krombholz, K., & Weippl, E. 2017. History of cryptographic currencies, *Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms*: 15-18: Springer.

Kawaguchi, N. 2019. Application of blockchain to supply chain: Flexible blockchain technology. *Procedia Computer Science*, 164: 143-148.

Kewell, B., Adams, R., & Parry, G. 2017. Blockchain for good? *Strategic change*, 26(5): 429-437.

Kietzmann, J., & Archer-Brown, C. 2019. From hype to reality: Blockchain grows up. *Business Horizons*, 62(3): 269-271.

Mehar, M. I., Shier, C. L., Giambattista, A., Gong, E., Fletcher, G., Sanayhie, R., Kim, H. M., & Laskowski, M. 2019. Understanding a revolutionary and flawed grand experiment in blockchain: the DAO attack. *Journal of Cases on Information Technology (JCIT)*, 21(1): 19-32.

Nakamoto, S. 2008. Bitcoin: A peer-to-peer electronic cash system.

Nisbet, R. 2017. History of the Idea of Progress: Routledge.

Noble, D. 1998. The religion of technology: The divinity of man and the spirit of invention: University of Toronto Press.

Notheisen, B., Hawlitschek, F., & Weinhardt, C. 2017. Breaking down the blockchain hype–towards a blockchain market engineering approach.

Ostrom, E. 1990. Governing the commons: The evolution of institutions for collective action: Cambridge university press.

Pärna, K. 2010. Believe in the net: Implicit religion and the internet hype, 1994-2001: Leiden University.

Pilkington, M. 2016. Blockchain technology: principles and applications, *Research handbook on digital transformations*: 225-253: Edward Elgar Publishing.

Saengchote, K. 2023. Decentralized lending and its users: Insights from Compound. *Journal of International Financial Markets, Institutions and Money*, 87: 101807.

Shapiro, A. L. 1999. The control revolution: How the Internet is putting individuals in charge and changing the world we know: Perseus Books.

Shin, L. 2022. The Cryptopians: Idealism, Greed, Lies, and the Making of the First Big Cryptocurrency Craze: Hachette UK.

Standage, T. 2005. The future of technology: John Wiley & Sons.

Swartz, L. 2018. What was Bitcoin, what will it be? The techno-economic imaginaries of a new money technology. *Cultural studies*, 32(4): 623-650.

Szabo, N. 1996. Smart contracts: building blocks for digital markets. *EXTROPY: The Journal of Transhumanist Thought,(16)*, 18(2): 28.

Szabo, N. 2005. Bit gold. Recuperado de https://nakamotoinstitute.org/bit-gold/TVer página: 251-260.

Ungureanu, P., & Cochis, C. 2023. Blockchain for good and the making of hype. How digital ventures and the media engage in technological prefigra-tion to co-construct hypes around emergent digital markets.

Ungureanu, P. 2025. "Running Code or Better Code? Expertise De/centralization Tensions in the Ethereum Blockchain Ecosystem".Research in the Sociology of Organizations, Special Issue on Expertise in and around Organizations.

Wood, G. 2014. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151(2014): 1-32.

Commoning by doing it yourself! Thoughts from the hackerspace and its passengers

Mickael Peiro[4]

In the 1990s, hackers began to think theoretically about developing hacking spaces to prove that they could be completely open about their work and ethics. The variety of names used by hacking communities reflects the diversity of the movement. While some groups and places that sound like hackerspaces don't want to be labeled as such because of the political resonance of the name, others proudly claim to be hackerspaces. The following lines are based on a doctoral journey and an ethnographic study of a hackerspace in France from 2016 to 2019. Far from being a place hidden from the world, the hackerspace brings together people who have decided to fight against technological accumulation and the hegemony of property, in a physical place that is visible and open to everyone. It is not meant to be a place for insiders, technophiles or only activists, but a place where everyone can meet and discuss issues freely and without constraints.

1. Draft Punk

In their struggle against proprietary technologies and standardized organizations, hackers have to walk the line between freedom and organization. But while they organize meetings to discuss the values and purpose of the space, at the same time - ... in the same place - ... these same hackers never stop 'doing'. They never stop replacing proprietary systems with free systems. They never stop setting up digital and electronic workshops to deconstruct technological complexity. They never stop giving beginner programming courses. They never stop teaching short-term travelers about astronomy, soap-making, and knot-tying. They never stop building online and physical libraries for as many people as possible. They never stop welcoming other alternative organizations and social movements. They never stop organizing conferences on the appropriation of techniques and technologies useful for the emancipation of all. They never stop opening their doors for meetings, demonstrations, presentations and friendly exchanges. They never stop offering a space for technological emancipation and digital survival.

Through 'doing', hackers continue and expand their struggle against property, managerialism, and technological hegemony, while relegating organization to last place. They see 'doing' as the sole purpose of the hackerspace. The governance spaces are not, and never have been, decision-making spaces, or even a particular moment where members with responsibilities within the space could meet to discuss future projects. Power, legitimacy and authority within the hackerspace have always been in the 'doing' and in all those who wish to embody it. Compared to corporate gatherings, meetings in hackerspaces have a very different ambition: to bring people together once again to discuss social issues freely, with the aim of promoting their emancipation. Unlike the other organizations it contests, the hackerspace does not divide the initiative into periods of reflection which would then lead to times for action, but maintains the existence of these spaces simultaneously, always giving decision-making power to those who do.

"There have always been a million theories about the content of the hackerspace. After that, everyone used it for what they needed, which is interesting, but doesn't make it a sustainable project. At the same time, it's interesting that the project wasn't completely written down from the start and that we didn't arrive with something, with rules to follow. It's important in terms of raising people's awareness that they themselves take part in the creation."

(Interview with a hacker).

The hackers' resistance to a dominant model is embodied in the creation of a site of experimentation that suggests a work in progress rather than a starting point or even a destination. The gathering of hackers is always complex to define the content and purpose of the place where hackers meet. It is the individuals who come to propose something that build the space. So, it's a space where individuals intertwine, for a moment or for a long time, to create something together. According to some members, there is a lack of usable equipment, lively workshops, pleasant premises, technical resources, and organization. The hackers experiment with technological and digital workshops as well as with organizational techniques. In addition, hackers construct a model that embodies their values and in which they would like to operate. It is this fabrication that could constitute the hackers' project. Not defined *a priori*, but constantly reloaded.

2. Host In The Shell

The place where hackers meet is very real, whilst the social transformation they are pursuing is at draft stage and the work still in progress. The hackerspace is having trouble sustaining its resources, and its activities still need to expand to reach more people and welcome more members. It could be that the purpose of the hackers is not just to challenge a dominant model, but to experiment with a different kind of space. While the members are sometimes torn between the desire to create a real place to develop projects and a technological support for social movements, they are not able to decide what ends the space should produce. They are also

[4] University of Toulouse. Laboratoire LGTO. mickael.peiro@iut-tlse3.fr

confused about the results for their members, for the civil society, for social movements and against the big digital companies.

The hackerspace thus achieves its most important results at the individual level. The members agree that the hackerspace is a proposal to others. The project is against the organizations monetize users' data, against the surveillance organized by companies and states, against the deprivation of users of their ability to appropriate technologies, but above all it is a place where 'doing' reigns. Hackers organize themselves to offer a place where people who want to participate in their emancipation can gather. The hackerspace is therefore a place created for citizens so that they themselves can contribute to their own emancipation. It's a place where kids come to learn the basics of coding, where teens come to 3D print replacement parts for their machines, and where adults come to modify their operating systems and encrypt their data. It's a place where people come to learn, but also to teach. Everyone can benefit from a shared space where all members of the hackerspace are involved collectively, even if they use the space individually.

"You only have to look at the people who turn up for the first time. You plug in three things, and they start an engine. You know they've done nothing, but for them, a world has opened up. It's certainly more interesting to do things while taking the piss and remaining open to everyone, than to start with a protest and then conform or not. That point is fatal. You have a situation where the framework is predefined, and the terms are already set. And you have another where you come in, you do cool things and I do cool things with you at the same time."

(Interview with a hacker).

The means that hackers use to promote the emancipation of citizens and to fight against dominant digital practices would become their ends. In the end, hackerspace residents, like the citizens who pass through its doors, never find a clear place (literally and metaphorically), be it against capitalism and private property, or for any form of freedom. What they do find is a place where they can study their own project and the shared space to understand how it works, modify and add to it, distribute it to other users and use it as they wish. This is how hackers think about commoning, by doing it themselves!