



Vaasan yliopisto  
UNIVERSITY OF VAASA

OSUVA Open  
Science

This is a self-archived – parallel published version of this article in the publication archive of the University of Vaasa. It might differ from the original.

## Blockchain Owns You: From Cypherpunk to Self-Sovereign Identity

**Author(s):** Serada, Alesha

**Title:** Blockchain Owns You: From Cypherpunk to Self-Sovereign Identity

**Year:** 2022

**Version:** Accepted manuscript

**Copyright** ©2022 The Rowman & Littlefield Publishing Group. All rights reserved. Please contact the publisher for permission to copy, distribute or reprint.

### **Please cite the original version:**

Serada, A. (2022). Blockchain Owns You: From Cypherpunk to Self-Sovereign Identity. In: Lushetich, N., Campbell, I. & Smith, D. (eds.) *Contingency and Plasticity in Everyday Technologies*, 53–70. Lanham: Rowman & Littlefield Publishers.  
<https://rowman.com/ISBN/9781538171578/Contingency-and-Plasticity-in-Everyday-Technologies>

# **Blockchain Owns You**

## **From Cypherpunk to Self-Sovereign Identity**

Alesha Serada

The technological term 'blockchain' became a common buzzword in the late 2010s. As of the 2020s, it is impossible to ignore the rise of blockchain technologies in emerging projects of digital identity and governance. In this chapter, I argue that these projects represent the reaction to invasive surveillance and algorithmic control in online environments. Moreover, this reaction is so acute that it shifts to another extreme, regressing to unambiguous personal identification and direct control in dystopian projects characterised by what I will call 'blockchain governmentality'. The repressive nature of such projects is often concealed behind the façade of democratic decision-making, but the voting is too easily manipulated, and the options are too few. Negotiable outcome is replaced with the finality of a pre-programmed decisions set in self-executable code. This mode of digital determinism is further reinforced by the immutability of historical records, the undeletability of personal data that is a feature of and not a bug in blockchain-based systems.

The core promise of blockchain is decentralisation. From the perspective of its early adopters, decentralisation meant personal sovereignty and horizontal participation in decision-making; new forms of governance were expected to evolve on this platform. At its most basic level, blockchain is a distributed electronic database that consists of chronologically organised, cryptographically protected immutable records – the ledger records of transactions between different parties such as exchanges of cryptocurrencies or other tokens like NFTs. The same ledger is simultaneously kept in many nodes of the network and periodically updated, usually painstakingly slowly, in some form of collective consensus between the multiple nodes that have the power of decision. The decentralisation of blockchain governance means that no single entity can control other nodes, only the ones to which it holds the keys.<sup>1</sup> Blockchain decentralisation affords multiplicity. In theory, it also affords direct democracy, if every node represents a person with the right to vote. There are two basic mechanisms of verification that support decentralised decision making, although both are open to technological and social exploits. Proof-of-work requires algorithmic 'mining' performed at large, factory-like, by time-and-energy-consuming private "mining farms."<sup>2</sup> Proof-of-stake, by contrast, gives the power of decision to the select few, typically those who hold big stakes in the appropriate cryptocurrency.<sup>3</sup> Both in fact defy the democratic promise of decentralisation,<sup>4</sup> however an elaborate discussion of this problem is beyond the scope of this chapter. While specific architectures of blockchain software solutions may be different, they have all inherited at least

some principles from the first popular blockchain software – Bitcoin.<sup>5</sup> The following generation of blockchain platforms is best represented by the most popular, although prohibitively expensive to use, Ethereum platform.<sup>6</sup> Ethereum has an added functionality in the form of ‘smart contracts,’ or self-executing programmes hosted in the nodes of the network. ‘Smart contracts’ are not, in fact, smart – and they are not even contracts,<sup>7</sup> – but we will return to this later.

Bitcoin and Ethereum are the most typical blockchains that possess many archetypical qualities<sup>8</sup>: network decentralisation, the immutability of past records, cryptographic security, transparency of some or all transactional data, and other, more conceptual than technological, features. One such feature is pseudonymity: most blockchain-based accounts have arbitrary names, and their users do not have to disclose their real-life identity in public. Initially, Bitcoin wallets were anonymous by design, but now personal identification is possible, and in fact easy, by forensic means. Almost every active blockchain user can be de-anonymised by scrapping data traces that connect the wallet to their named accounts. Besides, personal identification is required in most exchanges to convert cryptocurrencies into real-world money.<sup>9</sup> Even before the major cryptocurrency exchanges adopted Know Your Customer (KYC) policies, one of the early blockchain studies by Bill Maurer et al already noted that “[i]ts protocols offer not anonymity, but ‘pseudo-anonymity.’”<sup>10</sup> Later studies of crypto markets confirmed the performative nature of ‘pseudonymity’ and identity on blockchain, too.<sup>11</sup> The reversal of anonymity has been crucial in blockchain-based projects that verify and manage identities of natural and legal persons. To understand the problematic assumptions behind these projects, we need to pay closer attention to such (more conceptual than technological) features of blockchains as disintermediation and ‘trustlessness.’

Disintermediation means removing intermediaries such as banks and corporations from the interaction between parties that exchange money for services and goods.<sup>12</sup> Its liberating potential was discussed even before cryptocurrencies, in the virtual game items trade<sup>13</sup> – a highly speculative grey market with a high margin of risk. In a later development by Satoshi Nakamoto, disintermediation was a measure to protect merchants from dissatisfied customers, or at least, to optimise the costs of settling their claims.<sup>14</sup> This was Nakamoto’s reasoning behind making transactions irreversible, and their records immutable: neither party could abuse the payment system if they did not trust each other. Ideally, this meant the removal of the so-called unproductive beneficiaries, however also the removal of customer protection: everyone is their own bank with full financial responsibility for all their errors. ‘Trustlessness’ is a mode of operation in a decentralised and disintermediated trader network. It characterises transactions between parties who do not trust each other personally but need to interact none the less. The question of whether this is an absence of trust or a new kind of trust<sup>15</sup> – blind faith, to be more precise – is a discursive paradox specific to the community of blockchain users. To a blockchain enthusiast,<sup>16</sup> ‘trustlessness’ refers to the trust in the blockchain technology, rather than in people. This trust is often unconditional, or at least,

unshakeable by daily occurrences such as when this novel (and easily abused) technology fails.<sup>17</sup> However, as contemporary society is sliding into anomie in a manner similar to the beginning of the twentieth century<sup>18</sup> – blockchain may be the answer to this sorry spectacle.

Blockchain technologies represent powerful imaginaries in the international community of tech entrepreneurs.<sup>19</sup> They have inspired many utopian projects of blockchain governance based on the ‘code is law’ principle,<sup>20</sup> which originated in the techno-utopianism of early digital networks. In the words of Lawrence Lessig, “[t]his code, or architecture, sets the terms on which life in cyberspace is experienced.”<sup>21</sup> In her later critique, Wendy Hui Kyong Chun highlights the repressive character of such conceptualisations by rephrasing it as “code as law is code as police.”<sup>22</sup> In what follows, I examine representative projects of this kind through the lens of Foucaultian governmentality. The first section of the remainder of this chapter explains how digital society’s ‘algorithmic governmentality’ contributed to the emergence of the so-called ‘self-sovereign identity,’ – the project of the ‘digital self’ now habitually imagined on blockchain. In the second section, I examine what I term ‘blockchain governmentality’ using examples of ‘decentralised autonomous organisations’, or DAOs. ‘Blockchain governmentality’ is a way to imagine, design and, possibly, implement new forms of power relations in society by prioritising decentralised software architecture and self-executable machine code over the factual complexity of social relations. In the last section, I explain why blockchain governance should be considered deterministic: because it leads to less freedom – or to worse unfreedom – in terms of power and control.

## **THE ORIGINS OF BLOCKCHAIN GOVERNMENTALITY**

The concept of governmentality,<sup>23</sup> introduced by Michel Foucault, refers to a specifically European approach to government normalised in modernity. Pre-modern projects of governance, exemplified by the Machiavellian *Prince*, were focussed on taking control over a certain territory and maintaining it by “the right to kill”<sup>24</sup> (which is still the case with the Russian war against Ukraine in 2022). In contrast, in modern European governmentality, state power governs the population through indirect forms of governing (rather than through claiming territories and de-populating them with the aid of military force). This form of power is based on knowledge, not on force. As Johanna Oksala has observed, “[g]overnmentality implies the emergence of a particular, circular relationship between power and knowledge, or government and science.”<sup>25</sup> Governmentality is rational: it is a way of thinking about society as an object of governance. As modern society moved into its post-industrial, or informational phase, the practices of governance incorporated more ‘scientific’ means such as big data processing and predictive statistics. Conveniently, major informational corporations today obtain the so-called objective truths about the population from data voluntarily submitted by the internet users, however also from the digital traces they leave, often unknowingly, in

virtual environments,<sup>26</sup> in the form of cookies and browsing histories. This way of observing and modelling social reality can be described as “algorithmic governmentality.”<sup>27</sup> Drawing on Gilles Deleuze and Félix Guattari, Antoinette Rouvroy and Thomas Berns refer to “a certain type of (a)normative or (a)political rationality founded on the automated collection, aggregation and analysis of big data so as to model, anticipate and pre-emptively affect possible behaviours.”<sup>28</sup> While the previous, Panoptical, mode of surveillance implied human watchers, the data collected online is processed by machines capable of making decisions about individuals, such as whether they are allowed to cross the border,<sup>29</sup> or, in an authoritarian country, to travel at all.<sup>30</sup> The result is a regime of “dataveillance”<sup>31</sup> – a rather traditional model of Panopticon, now recreated by means of digital surveillance and automation. In a broader sense, governmentality is the rationalisation of governance through a variety of tactics: for example, applying statistics to make decisions about the wellbeing of a population. Blockchain governmentality is a socio-technological imaginary that seeks to rationalise fluid and often implicit relations of power and trust in society, codify and stabilise them with immutable ledgers and self-executing code. The practices of algorithmic and blockchain governmentality can be studied as a variation on the more general *#datapolitik*, defined as “a form of realpolitik of and by non-human agents.”<sup>32</sup> These non-human agents are represented by algorithms, in the first case, and by the so-called ‘smart contracts’ on blockchain, in the second.

## **SELF-SOVEREIGN IDENTITY: THE ONE-PERSON PANOPTICON**

Self-sovereign identity, or SSI, is a socio-technological imaginary that refers to the autonomous data subject, unambiguously attached to a natural person who shares only the data they wish to share about themselves. The most referred to SSI manifesto was authored by the software developer Christopher Allen.<sup>33</sup> Allen’s manifesto is a vision, not a technological concept, so paradoxes inevitably arise: appealing to the Cartesian ‘I,’ the manifesto describes singular, durable and portable digital identities where users fully control their data and online representation. These identities can exchange information across multiple systems and are issued independently of a centralised authority. The users’ rights are protected in conflicted situations, too. This appealing, if utopian, imaginary still inspires many blockchain projects. It is only natural to grow weary of ‘algorithmic governance’ and its statistical ‘regime of truth’ if one spends most of one’s time online. From this perspective, SSI symbolises resistance to the ‘algorithmic governmentality’ performed by major online platforms. Compared to the latter, decentralised blockchain platforms can indeed provide adequate cryptographic tools to limit access to personal data. However, their other affordances may not be as suitable. The core vision of SSI is that the user remains in full control of their own data – a worthy and timely goal under the condition of dataveillance.

However, this is not technically possible: this paradox comes from the nature of digital data, which is duplicated when shared. In the practice of SSI, some data are shared consensually upon request – for example, to log into another party’s system. To make this work, the other party is trusted to erase the received data from its own system after use. In practice, and especially in blockchain environments, this goes against the condition of ‘trustlessness,’ where parties are expected to act against each other’s best interests (otherwise they would not use blockchain).

The imaginary of a sovereign blockchain-based identity does not come from the technology itself, but from the philosophy of the crypto-anarchic ‘cypherpunk’ subculture that engendered Bitcoin,<sup>34</sup> only without the extraordinary digital literacy required to be a cypherpunk. The most publicly active organisation in the SSI space is at this point the non-profit blockchain alliance Sovrin Foundation.<sup>35</sup> Notably, the vision of this organisation is formulated as “Identity for All,”<sup>36</sup> which implies that one does not have a singular and unambiguous identity until they receive it from an institution such as Sovrin. This is as if “everyone on the planet wants and needs an identity in the form prescribed by the authorities, and that all that is required is a system to provide it.”<sup>37</sup> Many would argue that human beings have the (basic human) right to “life, liberty and security of person,”<sup>38</sup> regardless of their digital presence ‘in the system’. Sovrin’s agenda inspired the much-cited blockchain enthusiasts Michael Casey and Paul Vigna: from their perspective, SSIs are good because they “don’t depend on a government or a company to assert a person’s ID.”<sup>39</sup> Instead, such identities are expected to be verified by blockchains, which does not make practical sense: blockchain as a technology can only verify digital information that is native to blockchain.<sup>40</sup> Moreover, to forge a ‘native’ connection between a natural person and its digital identity, biometrics are commonly proposed,<sup>41</sup> which takes us back to even more invasive regimes of biopower, in Foucauldian terms. While it is technologically possible to build a privacy-friendly configuration of biometric identification where no data is shared with external parties,<sup>42</sup> it still remains to be seen whether blockchain adds value to such a configuration in terms of identity management. It could be that this technology’s affordance will steer blockchain in an even more dangerous direction, as we will see with another feature of blockchain: immutability.

## **IMMUTABILITY AS UNFREEDOM**

Immutability means that it is impossible to delete, forge or correct the record that has already been submitted to the block that secures the data; there are workarounds to fix it, but why would one, in that case, want it to be on blockchain in the first place? To satisfy the

wish to permanently register all citizens 'on the system,' blockchain-based identity systems lend themselves to various exercises in instrumental governmentality by actual human governments.<sup>43</sup> Such projects are already in development in a number of European countries, including The Netherlands,<sup>44</sup> Belgium,<sup>45</sup> Austria,<sup>46</sup> and Malta,<sup>47</sup> although still with some respect to personal freedom ensured by GDPR. Some of the state pilot projects in the USA include voting on blockchain.<sup>48</sup> Consequently, the real-life implementation of blockchain imaginaries engenders a very different manifestation of disintermediation: effectively, this means removing any mediator that could stand between the self and the state.

As soon as blockchain technology is used for the needs of centralised state control, projects of immutable, verifiable "permanent and portable digital identities"<sup>49</sup> bring back the most oppressive strategies of governmentality. The first impulse is always to test the creative solutionism of blockchain governmentality on refugees, who are seen as tokens for exercises of the technology businesses in "social good."<sup>50</sup> As the MIT scholars Cara Lapointe and Lara Fishbane suggest in their ethical framework for blockchain developers:

blockchain applications could provide the means to establish identities for individuals without identification papers, improve access to finance and banking services for underserved populations, and distribute aid to refugees in a more transparent and efficient manner.<sup>51</sup>

It is important to note that neither of these pilot projects has so far generated notable value for the people on whom they were tested.<sup>52</sup> The same holds true for other projects for social good, such as sustainability. In their review of technology-led experiments in sustainability governance, Nick Bernards et al conclude that experiments in blockchain-based democracy "are being developed and applied in ways that reinforce existing patterns of governance and relations of power."<sup>53</sup> Blockchain tends to reproduce, or even amplify, the existing asymmetries in owning and managing personal data. As Bernards et al show on the example of blockchain applications in Africa, "technological solutions to sustainability issues often boil down to attempts to render complex and geographically dispersed informal spheres of activity 'legible' and traceable."<sup>54</sup> This serves the needs of the controlling entities, such as investors and governments, rather than of those in need of help, which is similar to the above-mentioned critique voiced by Btihaj Ajana.<sup>55</sup>

Curiously, in the eyes of Lapointe and Fishbane, blockchain addresses "issues for underserved or marginalized people in ways that were previously unimaginable."<sup>56</sup> We should read this 'unimaginable' as a lack of imagination, if not something worse. One such unimaginable application is tracking refugees by scanning their irises to confirm their right to free food, a feature presented as good and useful by the developers of this disturbing pilot project, Building Blocks. In a much-cited paper by Fennie Wand and Primavera de Filippi, "refugees

only need to scan their irises at the point-of-sale to receive food assistance.”<sup>57</sup> My question is how little this ‘only’ actually means, and whether sharing surplus food with the most disadvantaged should subject these people to invasive biometric and algorithmic control. Ajana characterises this technocentric form of governmentality as “biometric humanitarianism;”<sup>58</sup> this is also how data-driven and biometric technologies are de facto used for “bordering,”<sup>59</sup> and for keeping displaced people outside of the digital state even when they are physically present on the state’s actual territory. Such practices are reminiscent of the most authoritarian disciplinarian practices and do not meet the actual needs of the displaced, the homeless, and the vulnerable. We tend to forget about workable solutions such as the Nansen passport – a temporary identity document issued by the League of Nations to refugees in 1922–1942, granting them the right to work in its member states<sup>60</sup> – and, surprisingly, did not require blockchain. Finally, the immutability of blockchain contradicts the fluidity and flexibility of social identities as well as their multiplicity: being a refugee is not an identity; it is the most vulnerable social status that should not be commemorated with an immutable record. In the end, Lapointe and Fishbane acknowledge that “immutability of information on Blockchain removes the ability to be forgotten,”<sup>61</sup> which also limits its applicability, at least in the EU projects of identity management. My guess would be that to leave it all behind is exactly what the most displaced, homeless, and more generally, marginalised subjects might desire.

## **‘SMART CONTRACTS’ AS THE PILLARS OF TRUSTLESSNESS**

‘Smart contracts’ are lightweight software programmes hosted on a blockchain platform, such as Ethereum. Typically, they are self-executable, when triggered by a message or a certain state of the system, and almost impossible to change after they have been deployed. A combination of smart contracts constitutes a decentralised application (DAPP). Andrea Pinna et al describe a thriving community of coders in the programming language Solidity, used to create smart contracts on Ethereum; the most common applications are decentralised finance apps and blockchain-based games.<sup>62</sup> The term ‘smart contracts’ causes a lot of confusion in the community of blockchain users, who imagine them as the legal manifestation of the ‘code is law’ principle<sup>63</sup>. Indeed, Pinna et al describe a particular, although significantly less used, category of ‘smart contracts.’ These are ‘notary contracts’ that codify agreements between parties and turn them into self-executable programmes. Again, smart contracts are not legal contracts – they are self-executing programmes that do what their programmers tell them to do. The output of these programmes is only legal if accompanied by an actual contract in a legally accepted form.<sup>64</sup> This remains the case even when countries, such as Malta, partially integrate ‘smart contracts’ into their legal framework.<sup>65</sup>

Blockchain-based governance is often imagined in the form of Decentralised Autonomous Organizations (DAOs) – communities that manage themselves and the projects they



collectively develop by technological means afforded by blockchain. Some aspects of governance, such as managing the collective property of the project, can be automated and inscribed in smart contracts.<sup>66</sup> Blockchain-based tokens can be used for voting in certain forms of direct democracy.<sup>67</sup> DAO as a form of collective governance was introduced in the Ethereum White paper, which described “long-term smart contracts that contain the assets and encode the bylaws of an entire organization.”<sup>68</sup> However, the Ethereum DAO that was organised following these principles also became the first example of a major-scale fraud on the cryptocurrency market.<sup>69</sup> While many blockchain projects today label themselves as DAOs, successful examples of long-term self-governance are yet to be seen, and it may be the right time to ask why. There is no shortage of democratic governance projects on blockchain today. A typical blueprint used in many such projects can be found, for example, in the paper by Vijay Mohan, who sees the main reason for academic misconduct in the increased competition for publications and funding, and yet suggests to solve the problem with ‘tokenomics’ and reputation tokens (which, upon second thought, would further intensify the competition and create black market for such tokens).<sup>70</sup> Just to name a few least self-contradictory examples: in his exploration of ‘fully-automated liberalism’, Bernhardt Reinsberg presents a utopian project of climate governance on blockchain in the form of a DAO;<sup>71</sup> Artyom Kosmarski explores how science and academic research can be governed in a decentralised way;<sup>72</sup> Morshed Mannan envisions a workers’ cooperative in the form of a DAO.<sup>73</sup> However, even the most productive discussions of DAOs – as the future form of self-organisation – miss a crucial point. In all these cases, transparency, immutability, and automation via smart contracts are trusted above trusting the actual people and organisations that, by themselves, should constitute social changes. Blockchains are used to create non-negotiable binding agreements in place of relationships based on good will and shared ideals in the real world. This constitutes distrust, not trustlessness. Finally, governance with smart contracts brings back the same problem of *#datapolitik* that has already been discussed in the context of ‘algorithmic governmentality’:<sup>74</sup> only before, the rule of algorithms was indirect and implicit, and could be negotiated by most ‘algorithmically aware’ data subjects.<sup>75</sup> Being ‘smart’ is no longer about anticipating the needs of the internet users. Today, it is about the acceptable tyranny of programmes over people. With ‘smart contracts’ on blockchain, “non-human, sovereign agents”<sup>76</sup> are officially assigned as managers and judges of human behaviour in automated systems.<sup>77</sup> Furthermore, they are entitled to govern reality itself, without the need to check back with the said reality.

## **BLOCKCHAIN GOVERNANCE AS NEW FEUDALISM**

I have already mentioned the confusion between smart contracts and legal contracts. There is one more confusion to untangle: when blockchain enthusiasts speak of DAOs, they imagine smart contracts as a manifestation of the social contract. Their imaginaries of decentralised government usually repeat the principles of direct democracy described by Jean-Jacques

Rousseau in 1762; in Rousseau's words, "this act of association creates a moral and collective body, composed of as many members as the assembly contains votes, and receiving from this act its unity, its common identity, its life and its will."<sup>78</sup> However, unlike the voluntary and implicit social contract in Rousseau's idealistic project, smart contracts are externally deployed, technologically unbreakable, and imposed by the developers of the software system. Even in the perfect and most reasonable implementation (yet to be observed 'in the wild' of blockchain communities), all power is delegated to the machines. Only now these machines do not even collect a digital dossier on their subjects – they reward and punish their behaviour based on pre-defined rules and simply apply them to 'flocks of humans', like flocks of sheep, without wasting any resources on recognising their identity (subjectivity) as the most basic and archaic form of 'pastoral power' that preceded modern governmentality.<sup>79</sup> In this way, blockchain governance projects use the most reactionary model of the Panopticon: Vigna and Casey even unironically praise "the God's-eye view" that blockchain provides.<sup>80</sup> They may encourage communities to actively evaluate the worth of each member and reward or punish them by public voting on blockchain – as in a now reorganised social network Steem,<sup>81</sup> one of the most active projects of collective blockchain governance. Compare this to Foucault's Panopticon in its most radical and archaic form: "[y]ou have an apparatus of total and circulating mistrust, because there is no absolute point. The perfected form of surveillance consists in a summation of malveillance."<sup>82</sup> These communities may promise direct democracy of the Rousseauian kind, however such democracy is predicated on Panoptical surveillance. Foucault would call it an illusion:

It is the illusion of almost all of the eighteenth-century reformers who credited opinion with considerable potential force. Since opinion could only be good, being the immediate consciousness of the whole social body, they thought people would become virtuous by the simple fact of being observed.<sup>83</sup>

However, while blockchain adopters are aware that every transaction they make remains on blockchain forever, this does not make them virtuous. Everything is permitted in the environment of trustlessness, 'as long as it is technically possible, because all trust is now delegated to code,<sup>84</sup> and 'code is law.'<sup>85</sup> Again, regardless of blockchain, Chun characterises the same scenario as "a decay of the decay that is democracy."<sup>86</sup>

## **CONCLUSION: BLOCKCHAIN GOVERNMENTALITY**

Algorithmic and blockchain governmentality represent two different forms of *#realpolitik*, whose "aim is no longer to exclude anything that does not fit the average but to avoid the unpredictable, to make sure that everybody is truly themselves."<sup>87</sup> Algorithmic governmentality sees this truth as the product of auto-learning algorithms that devour real-life data in real time. Blockchain governmentality offers a different, and very literal and

transparent, regime of 'digital truth.' Every record on blockchain is cryptographically secured and cannot be changed, unless a new version ('fork') of blockchain is created, or the voting majority (typically of 51%) is controlled of a single entity (the former scenario is much more common than the latter). This conceptual (even if not always factual) immutability stands for 'truth' in the Vigna and Casey's widely used metaphor of blockchain as the 'truth machine.'<sup>88</sup> In light of this anxiety, self-sovereign identities are a barely masked attempt to identify and discipline others, not oneself. In addition, algorithmic and blockchain governance implements a variety of means to achieve the shared goal to de-subjectify the individual. Apart from possibly malicious intermediaries (whose danger and involvement may be overestimated), disintermediation also removes the intricate relation between the natural human, their data subject or data subjects, and the apparatus of control. The removal of intermediaries simultaneously establishes the blockchain network as the only unquestionable authority, the one that cannot be fooled by managing multiple personas or performing 'pretend' searches to trick the algorithm. The most disturbing effect of *#datapolitik*, potentially amplified in blockchain solutions, is that when non-human agents take control and make decisions about human subjects, human subjects lose their agency and even subjectivity. The subject is here rigidly, or even immutably, fixed at its designated location in the node network, and eventually becomes the property of the network, ruled by non-negotiable self-executing programmes.

Blockchain inventors are well aware of the technology's flaws. This, however, does not quell their urge to register homeless people on blockchain so they can get free food, likely because of the typical impulse of every inventor: 'let's try it (on others) and see what happens.' This urge is what makes it 'interesting,' alongside a lack of empathy with the people to whom future blockchain solutions will be applied. By equating the individual with their data subject, blockchain governmentality downgrades to the previous regime of direct, unmediated discipline executed on one's physical body. In blockchain governmentality, there is no relation between the individual and the state. Verified by a supposedly indestructible record, one becomes one's own profile, and this, I would argue, is where blockchain governmentality wants us. Governing is outsourced to 'the code is law' principle; and, in fact, as of 2021, 51% of European and 31% of British respondents supported replacing parliamentary seats with robots in the survey by IE University.<sup>89</sup>

Despite claims to decentralisation and democratisation, blockchain affordances support a very particular power fantasy, and a very individualist one. Even before and beyond blockchain, "code resuscitates fantasies of sovereign, or executive, structures of power," in Chun's interpretation of Judith Butler's work.<sup>90</sup> When a technology innovator or a researcher proposes another project of governance, they adopt the perspective of those who govern, rather than those who are governed (understandably so, as such inventors are typically

comfortable with their own privileges of prestigious education and career). This is particularly striking in utopian projects of democratic governance on blockchain such as Decentralised Autonomous Organizations. When in a position where external governance becomes visible and sensible, projects of personal autonomy are suggested, as we can see in the example of self-sovereign identity. Both of these two modes of blockchain governmentality ignore the multilateral direction and inherent asymmetry of governance, which always includes relations of governing and being governed, by the forces and impulses that come from outside and from within.

Initially, blockchain technologies promised decentralisation, anonymity, transparency, verifiability, the removal of unproductive intermediaries, security, and trust. All these promises have long been broken or twisted, but the last crucial feature, immutability, remains, well... immutable. Its most inviting application is to produce undisputed historical truth about the past and the present of an object, human or a non-human entity. A blockchain-based subject writes their future with every deed, and this future, as well as the past, cannot be rewritten. When used for data integration across business and social networks, blockchain technology becomes the ultimate '*de-Terminator*,' which poses the direct threat to the project of the self by limiting its future to options immutably secured on blockchain and prescribed in self-executing rules of governance. Furthermore, when collectively materialised in the form of DAOs or similar '*social bodies*,' blockchain governance creates new hegemony in the form of stakeholders, who are either the first ones to adopt a certain solution as well as the ones who own most of its tokens, which gives them voting and decision rights, or, most typically, both at once. On a theoretical level, it equates this new governmentality with the technocentric "Californian ideology"<sup>91</sup> that privileges wealthy 'First-world' citizens. To showcase the 'rags to riches' principle, this ideology may also employ the lucky few token 'self-made people' who serve as the 'model workers' of the new blockchain economy.<sup>92</sup> This technocentric meritocracy, however, is famously exclusive or ignorant. In the majority of cases, immutability, transparency and irreversibility may radically limit what Foucault called the "work carried out by ourselves upon ourselves as free beings"<sup>93</sup> that characterises the (post) modern individual.

---

<sup>1</sup> See, for example, Joshua Ellul et al., "Regulating Blockchain, DLT and Smart Contracts: A Technology Regulator's Perspective," *ERA Forum* 21 (June 30, 2020), 209–20, doi: 10.1007/s12027-020-00617-7.

<sup>2</sup> As in "MASSIVE Crypto Mining Farm Tour | Bitcoin, Dash, and GPU Mining!," *Deeper in the Mines* (VoskCoin, February 10, 2020), <https://www.youtube.com/watch?v=4ekOeDG2D8E>.

<sup>3</sup> "Ethereum Proof of Stake," *EthHub*, accessed July 26, 2020, <https://docs.ethhub.io/ethereum-roadmap/ethereum-2.0/proof-of-stake/>.

<sup>4</sup> Irni Eliana Khairuddin and Corina Sas, "An Exploration of Bitcoin Mining Practices: Miners' Trust Challenges and Motivations," *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19* (the 2019 CHI Conference, Glasgow, Scotland, UK: ACM Press, 2019), 1–13, doi: 10.1145/3290605.3300859; Sarah Azouvi, Mary Maller, and Sarah Meiklejohn, "Egalitarian Society or Benevolent Dictatorship: The State of Cryptocurrency Governance," *Financial Cryptography Workshops* (2018), doi: 10.1007/978-3-662-58820-8\_10.

<sup>5</sup> Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

- <sup>6</sup> Vitalik Buterin, “Ethereum White Paper. A Next Generation Smart Contract & Decentralized Application Platform,” 2013, <https://ethereum.org/en/whitepaper/>.
- <sup>7</sup> Kelvin F. K. Low and Eliza Mik, “Pause the Blockchain Legal Revolution,” *International and Comparative Law Quarterly* 69, no. 1 (January 2020): 135–75, doi: 10.1017/S0020589319000502.
- <sup>8</sup> See e.g. Cara Lapointe and Lara Fishbane, “The Blockchain Ethical Design Framework,” *Innovations: Technology, Governance, Globalization* 12, no. 3–4 (January 2019): 50–71, doi: 10.1162/inov\_a\_00275.
- <sup>9</sup> EU has banned anonymous crypto wallets and transactions altogether: Huw Jones and Tom Wilson, “EU Lawmakers Back New Tracing Rule for Crypto Transfers,” *Reuters*, March 31, 2022, sec. Europe, <https://www.reuters.com/world/europe/eu-lawmakers-back-new-tracing-rule-crypto-transfers-2022-03-31/>.
- <sup>10</sup> Bill Maurer, Taylor C. Nelms, and Lana Swartz, “‘When Perhaps the Real Problem Is Money Itself’: The Practical Materiality of Bitcoin,” *Social Semiotics* 23, no. 2 (April 2013): 261–77, doi: 10.1080/10350330.2013.777594.
- <sup>11</sup> Angus Bancroft and Peter Scott Reid, “Challenging the Techno-Politics of Anonymity: The Case of Cryptomarket Users,” *Information, Communication & Society* 20, no. 4 (April 3, 2017): 497–512, doi: 10.1080/1369118X.2016.1187643.
- <sup>12</sup> Paul Vigna and Michael J. Casey, *The Truth Machine: The Blockchain and the Future of Everything* (New York: St. Martin’s Press, 2018); Lapointe and Fishbane, “The Blockchain Ethical Design Framework.”
- <sup>13</sup> Dan Hunter and F. Gregory Lastowka, “Amateur-to-Amateur,” *William and Mary Law Review* 46, no. 3 (2004): 951–1030.
- <sup>14</sup> Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System.”
- <sup>15</sup> Angela Walch, “In Code(Rs) We Trust: Software Developers as Fiduciaries in Public Blockchains,” in *The Blockchain Revolution: Legal and Policy Challenges* (Oxford, UK: Oxford University Press, 2018), doi: 10.1093/oso/9780198842187.003.0004.
- <sup>16</sup> See Melanie Swan, *Blockchain: Blueprint for a New Economy* (Sebastopol, CA: O’Reilly Media, 2015); Vigna and Casey, *The Truth Machine*; Primavera de Filippi and Aaron Wright, *Blockchain and the Law: The Rule of Code* (Cambridge, MA: Harvard University Press, 2018).
- <sup>17</sup> See, for example, Gili Vidan and Vili Lehdonvirta, “Mine the Gap: Bitcoin and the Maintenance of Trustlessness,” *New Media & Society* 21, no. 1 (January 2019): 42–59, doi: 10.1177/1461444818786220.
- <sup>18</sup> “It is to this state of anomie that, as we shall show, must be attributed the continually recurring conflicts and disorders of every kind of which the economic world affords such a sorry spectacle,” Emile Durkheim, *The Division of Labor in Society* (New York: Simon and Schuster, 2014).
- <sup>19</sup> Arnoud Lagendijk et al., “Blockchain Innovation and Framing in the Netherlands: How a Technological Object Turns into a ‘Hyperobject,’” *Technology in Society* 59 (November 1, 2019): 1–10, doi: 10.1016/j.techsoc.2019.101175; Yong Ming Kow and Caitlin Lustig, “Imaginarities and Crystallization Processes in Bitcoin Infrastructuring,” *Computer Supported Cooperative Work (CSCW)* 27, no. 2 (April 2018): 209–32, doi: 10.1007/s10606-017-9300-2; Moritz Becker, “Blockchain and the Promise (s) of Decentralisation : A Sociological Investigation of the Sociotechnical Imaginaries of Blockchain,” *Proceedings of the STS Conference Graz*, 2019, 6–30, doi: 10.3217/978-3-85125-668-0-02.
- <sup>20</sup> Walch, “In Code (Rs) We Trust.”
- <sup>21</sup> Lawrence Lessig, “Code Is Law: On Liberty in Cyberspace.” *Harvard Magazine*, 2000. <https://www.harvardmagazine.com/2000/01/code-is-law-html>.
- <sup>22</sup> Wendy Hui Kyong Chun, *Updating to Remain the Same: Habitual New Media* (Cambridge, MA: MIT Press, 2017), 82.
- <sup>23</sup> Michel Foucault, *Security, Territory, Population: Lectures at the College De France, 1977 - 78*, (London, UK: Palgrave Macmillan, 2007).
- <sup>24</sup> Johanna Oksala, “From Biopower to Governmentality,” in *A Companion to Foucault*, ed. Christopher Falzon, Timothy O’Leary, and Jana Sawicki (Chichester, UK: John Wiley & Sons, Ltd, 2013), 320–36, doi: 10.1002/9781118324905.ch15.
- <sup>25</sup> Oksala, 362.
- <sup>26</sup> Antoinette Rouvroy and Thomas Berns, “Algorithmic Governmentality and Prospects of Emancipation,” *Réseaux* 177, no. 1 (October 14, 2013): 163–96.
- <sup>27</sup> Ibid.
- <sup>28</sup> Ibid. 173.
- <sup>29</sup> Btihaj Ajana, “Biometric Datafication in Governmental and Personal Spheres,” in *Big Data—A New Medium?* (Oxfordshire, UK: Routledge, 2020), 63–79.
- <sup>30</sup> Chuncheng Liu, “Multiple Social Credit Systems in China,” *Economic Sociology: The European Electronic Newsletter* 21, no. 1 (2019): 22–32.
- <sup>31</sup> Rouvroy and Berns “Algorithmic Governmentality and Prospects of Emancipation,” 169.
- <sup>32</sup> Çağlar Köseoğlu and Davide Panagia, “#datapolitik: An Interview with Davide Panagia,” *Contriver’s Review*, November 14, 2017.

- 
- <sup>33</sup> Christopher Allen, “The Path to Self-Sovereign Identity,” April 25, 2016, <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>.
- <sup>34</sup> Henrik Karlström, “Do Libertarians Dream of Electric Coins? The Material Embeddedness of Bitcoin,” *Distinktion: Journal of Social Theory* 15, no. 1 (January 2, 2014): 23–36, doi: 10.1080/1600910X.2013.870083; Enrico Beltramini, “The Cryptoanarchist Character of Bitcoin’s Digital Governance,” *Anarchist Studies* 29, no. 2 (2021): 75–99, doi: 10.3898/AS.29.2.03.
- <sup>35</sup> Sovrin Foundation, “Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust,” January 2018, <https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf>.
- <sup>36</sup> Sovrin Foundation.
- <sup>37</sup> Ajana, “Biometric Datafication in Governmental and Personal Spheres.”
- <sup>38</sup> United Nations General Assembly. *Universal Declaration of Human Rights: Proclaimed by the United Nations General Assembly, Paris, December 1948*. Oxford, UK: Bodleian Library, 2021.
- <sup>39</sup> Vigna and Casey, *The Truth Machine*, 8.
- <sup>40</sup> Laura Gonzalez, “Blockchain, Herding and Trust in Peer-to-Peer Lending,” *Managerial Finance* 46, no. 6 (January 1, 2019): 815–31, doi: 10.1108/MF-09-2018-0423; Kelvin F. K. Low and Eliza Mik, “Pause the Blockchain Legal Revolution”.
- <sup>41</sup> Applied Recognition and Sovrin Foundation, “Applied Recognition and Sovrin Foundation Announce Cooperation On...” (Toronto: PRWeb, April 19, 2021), <https://www.prweb.com/releases/2021/04/prweb17871399.htm>; J. S. Hammudoglu et al., “Portable Trust: Biometric-Based Authentication and Blockchain Storage For Self-Sovereign Identity Systems” (2017), <https://arxiv.org/pdf/1706.03744>; Margie Cheesman, “Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity,” *Geopolitics*, October 4, 2020, 1–26, doi: 10.1080/14650045.2020.1823836; Fennie Wang and Primavera De Filippi, “Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion,” *Frontiers in Blockchain* 2 (2020), doi: 10.3389/fbloc.2019.00028.
- <sup>42</sup> see e.g. Chen Tai Pang et al., “Biometric System-on-Card,” in *Encyclopedia of Biometrics*, ed. Stan Z. Li and Anil K. Jain (Boston, MA: Springer US, 2009), 1–6, doi: 10.1007/978-3-642-27733-7\_9136-1.
- <sup>43</sup> Dutch Blockchain Coalition, “Co-Write Self-Sovereign Identity’s Next Chapter,” *Dutch Blockchain Coalition* (blog), 2020, <https://dutchblockchaincoalition.org/en/news/co-write-self-sovereign-identity-next-chapter>.
- <sup>44</sup> Dutch Blockchain Coalition.
- <sup>45</sup> Microsoft, “How a Decentralized Identity and Verifiable Credentials Can Streamline Both Public and Private Processes,” March 17, 2021, <https://customers.microsoft.com/en-us/story/1351115614634143059-flanders-government-of-belgium-government-azure-active-directory>.
- <sup>46</sup> Ralf-Roman Schmidt, Roman Geyer, and Pauline Lucas, “Discussion Paper. The Barriers to Waste Heat Recovery and How to Overcome Them?” (Austrian Institute of Technology, June 2020), <https://www.euroheat.org/wp-content/uploads/2020/06/Discussion.pdf>.
- <sup>47</sup> Ellul et al., “Regulating Blockchain, DLT and Smart Contracts.”
- <sup>48</sup> Sunoo Park et al., “Going from Bad to Worse: From Internet Voting to Blockchain Voting,” *Journal of Cybersecurity* 7, no. 1 (February 16, 2021): 1–15, doi: 10.1093/cybsec/tyaa025.
- <sup>49</sup> Lapointe and Fishbane, “The Blockchain Ethical Design Framework.”
- <sup>50</sup> See also Ajana, “Biometric Datafication in Governmental and Personal Spheres.”
- <sup>51</sup> Lapointe and Fishbane, “The Blockchain Ethical Design Framework.”
- <sup>52</sup> Cheesman, “Self-Sovereignty for Refugees?”
- <sup>53</sup> Nick Bernards et al., “Interrogating Technology-Led Experiments in Sustainability Governance,” *Global Policy*, 2020, doi: 10.1111/1758-5899.12826.
- <sup>54</sup> Bernards et al.
- <sup>55</sup> Ajana, “Biometric Datafication in Governmental and Personal Spheres.”
- <sup>56</sup> Lapointe and Fishbane, “The Blockchain Ethical Design Framework.”
- <sup>57</sup> Wang and De Filippi, “Self-Sovereign Identity in a Globalized World”; see also Vigna and Casey, *The Truth Machine* who start their book with an enthusiastic description of registering refugees on blockchain.
- <sup>58</sup> Ajana, “Biometric Datafication in Governmental and Personal Spheres.”
- <sup>59</sup> Ajana. Anecdotally, the author of this chapter had one of the most terrifying experiences in their life when they almost failed fingerprint recognition in the EU VIS system that controls migration, due to intensive guitar practice having altered their fingerprints.
- <sup>60</sup> Otto Hieronymi, “The Nansen Passport: A Tool of Freedom of Movement and of Protection,” *Refugee Survey Quarterly* 22, no. 1 (2003): 36–47.
- <sup>61</sup> Lapointe and Fishbane, “The Blockchain Ethical Design Framework.”

- 
- <sup>62</sup> Andrea Pinna et al., “A Massive Analysis of Ethereum Smart Contracts Empirical Study and Code Metrics,” *IEEE Access* 7 (2019): 78194–213, doi: 10.1109/ACCESS.2019.2921936.
- <sup>63</sup> de Filippi and Wright, *Blockchain and the Law: The Rule of Code*, 72-88.
- <sup>64</sup> Kelvin F. K. Low and Eliza Mik, “Pause the Blockchain Legal Revolution”.
- <sup>65</sup> Laura Camilleri, “Blockchain-Based Smart Contracts’ Legal Enforceability in Malta and the UK: A Square Peg in a Round Hole?” (LLM in International Corporate and Commercial Law, University of York, 2019); Joshua Ellul et al., “Regulating Blockchain, DLT and Smart Contracts: A Technology Regulator’s Perspective”.
- <sup>66</sup> See e.g. ArkDev, “Gray Boys Whitepaper,” 2021.
- <sup>67</sup> See e.g. Barbara Guidi, Andrea Michienzi, and Laura Ricci, “Analysis of Witnesses in the Steem Blockchain,” *Mobile Networks and Applications*, April 14, 2021, doi: 10.1007/s11036-021-01749-x.
- <sup>68</sup> Buterin, “Ethereum White Paper.”
- <sup>69</sup> Quinn DuPont, “Experiments in Algorithmic Governance: An Ethnography of ‘The DAO,’ a Failed Decentralized Autonomous Organization,” in *Bitcoin and Beyond: The Challenges and Opportunities of Blockchains for Global Governance*, ed. Malcolm Campbell-Verduyn (New York: Routledge, 2018), 157–77; Walch, “In Code(Rs) We Trust.”
- <sup>70</sup> Vijay Mohan, “On the Use of Blockchain-Based Mechanisms to Tackle Academic Misconduct.” *Research Policy* 48, no. 9 (November 1, 2019). doi: 10.1016/j.respol.2019.103805.
- <sup>71</sup> Bernhard Reinsberg, “Fully-Automated Liberalism? Blockchain Technology and International Cooperation in an Anarchic World.” *International Theory*, 2020, doi: 10.1017/S1752971920000305.
- <sup>72</sup> Artyom Kosmarski, “Blockchain Adoption in Academia: Promises and Challenges,” *Journal of Open Innovation: Technology, Market, and Complexity* 6, no. 4 (December 2020): 117, doi: 10.3390/joitmc6040117.
- <sup>73</sup> Morshed Mannan, “Fostering Worker Cooperatives with Blockchain Technology: Lessons from the Colony Project.” *Erasmus Law Review* 11, no. 3 (2018): 190–203, doi: 10.5553/ELR.000113.
- <sup>74</sup> Köseoğlu and Panagia, “#datapolitik.”
- <sup>75</sup> Erin Klawitter and Eszter Hargittai, “‘It’s Like Learning a Whole Other Language’: The Role of Algorithmic Skills in the Curation of Creative Goods,” *International Journal of Communication* 12, (September 13, 2018): 21, <https://ijoc.org/index.php/ijoc/article/view/7864>; Shagun Jhaver, Yoni Karpfen, and Judd Antin, “Algorithmic Anxiety and Coping Strategies of Airbnb Hosts,” *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18* (2018 CHI Conference, Montreal QC, Canada: ACM Press, 2018), 1–12, doi: 10.1145/3173574.3173995.
- <sup>76</sup> Köseoğlu and Panagia, “#datapolitik.”
- <sup>77</sup> See e.g. Melanie Swan, “Transhuman Crypto Cloudminds,” in *The Transhumanism Handbook*, ed. Newton Lee (Cham: Springer International Publishing, 2019), 513–27, doi: 10.1007/978-3-030-16920-6\_33.
- <sup>78</sup> Jean-Jacques Rousseau, *On the Social Contract* (South Bend, IN: St. Augustine Press, 2018).
- <sup>79</sup> Oksala, “From Biopower to Governmentality.”
- <sup>80</sup> Vigna and Casey, *The Truth Machine*, 20.
- <sup>81</sup> Raffaele Fabio Ciriello, Roman Beck, and Jason Thatcher, “The Paradoxical Effects of Blockchain Technology on Social Networking Practices” (*Thirty Ninth International Conference on Information Systems*, San Francisco, CA, USA, 2018).
- <sup>82</sup> Michel Foucault, *Power/Knowledge: Selected Interviews and Other Writings, 1972-1977* (New York: Pantheon Books, 1980), 158.
- <sup>83</sup> Foucault, *Power/Knowledge*, 161.
- <sup>84</sup> Vidan and Lehdonvirta. “Mine the Gap: Bitcoin and the Maintenance of Trustlessness.”
- <sup>85</sup> Lessig, “Code Is Law: On Liberty in Cyberspace.”. See also: de Filippi and Wright, *Blockchain and the Law: The Rule of Code*.
- <sup>86</sup> Chun, *Updating to Remain the Same: Habitual New Media*, 83.
- <sup>87</sup> Rouvroy, Berns, and Libbrecht, “Algorithmic Governmentality and Prospects of Emancipation,” 172.
- <sup>88</sup> Vigna and Casey, *The Truth Machine*.
- <sup>89</sup> Center for the Governance of Change. “IE University Research on Replacing MPs with Robots.” *IE University* (blog). Accessed April 28, 2022. <https://www.ie.edu/university/news-events/news/ie-university-research-reveals-1-2-europeans-want-replace-national-mps-robots/>.
- <sup>90</sup> Chun, *Updating to Remain the Same: Habitual New Media*, 83.
- <sup>91</sup> Richard Barbrook and Andy Cameron, “The Californian Ideology,” *Science as Culture* 6, no. 1 (January 1, 1996): 44–72, doi: 10.1080/09505439609526455.
- <sup>92</sup> Ciriello, Beck, and Thatcher, “The Paradoxical Effects of Blockchain Technology on Social Networking Practices.”
- <sup>93</sup> Michel Foucault, “What Is Enlightenment?,” in *The Foucault Reader* (New York: Pantheon Books, 1984), 32-50.