Blockchain, GDPR, and fantasies of data sovereignty

Blockchain, GDPR, and Fantasies of Data Sovereignty

Dr Robert Herian
Senior Lecturer in Law
The Open University

robert.herian@open.ac.uk
https://orcid.org/0000-0001-7001-7578

Keywords: Blockchain; Data; GDPR; Regulation; Fantasy; Control; Sovereignty

ABSTRACT

Like the European Union's General Data Protection Regulation (GDPR), the broader, mainstream emergence of blockchain technology in the present moment of, what I call, *data dysphoria* is no accident. It is in part reaction to data dysphoria, and in part exploitation of it, a duality underpinned by the tantalizing promise of the prosumer 'taking control' of their data and establishing sovereignty over it. Blockchain and GDPR alike aim to resolve 'problem'/'solution' matrices with deep roots in a wide variety of global economic, political, social, legal and cultural contexts. This article explores the problem of achieving resolution based on innovation and technology by offering an account of the rise of blockchain and implementation of GDPR within a psycho-political framework, one in which fantasies of taking control are predominant yet highly contestable actualities in the lives of technology users.

1 INTRODUCTION

To be data sovereign is to take control of one's personal digital destiny. This is the tantalizing and powerful idea that the European Union's General Data Protection Regulation (GDPR) and a variety of blockchain applications promote[1]. It is an idea formed not simply around practices of individual data self-care maintained through combinations of network applications and the assertion of rights, but encompasses a whole range of economic, political and social concerns and motivations. Yet it is an idea that arguably

[1] See, for example, s.5, s.6, and s.7 of the GDPR:

(5)The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows of personal data. The exchange of personal data between public and private actors, including natural persons, associations and undertakings across the Union has increased. National authorities in the Member States are being called upon by Union law to cooperate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State.

(6)Rapid technological developments and globalisation have brought new challenges for the protection of personal data. The scale of the collection and sharing of personal data has increased significantly. Technology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities. Natural persons increasingly make personal information available publicly and globally. Technology has transformed both the economy and social life, and should further facilitate the free flow of personal data within the Union and the transfer to third countries and international organisations, while ensuring a high level of the protection of personal data.

(7)Those developments require a strong and more coherent data protection framework in the Union, backed by strong enforcement, given the importance of creating the trust that will allow the digital economy to develop across the internal market. Natural persons should have control of their own personal data. Legal and practical certainty for natural persons, economic operators and public authorities should be enhanced.

assumes the retreat or abject failure of social mechanisms and institutions, including intersubjective trust, and does so, I argue, not for the purposes of recalibrating or reinvigorating social cohesion, cultural interaction, or political integrity, but in order to enhance economic self-determination within the terms of neoliberal capitalism[2].

This essay will begin by exploring what I call *data dysphoria*, a type of unease manifest in cyberspace which can be attributed to mass proliferations of personal data online, as well as increasing consumer concerns over the management and mismanagement of data by commercial actors. Equally, however, this unease follows complex psychological negotiations between data subjects and the systems and networks they engage with, which give rise to fantasies of control conducted through an array of different legal and technological mechanisms, namely, GDPR and blockchain applications, both of which promote enhanced levels of individual data management. Further, the compatibility of certain rights under GDPR will be discussed in light of the emergence of blockchain applications with the aim of assessing the level of entanglement and compatibility between GDPR and blockchain. This essay will argue that whilst convergence, paradox and perhaps even conflict describe the relationship and cursory interlinking of the key characteristics of GDPR and blockchain applications and implementations, both are ultimately defined by fantasies of data sovereignty symptomatic of a growing data dysphoria within and outside cyberspace.

Analyses such as the one conducted in this essay are not marginal to the formal business of law and regulation, but necessary for ascertaining *what lies beneath* stakeholder

[2] Given GDPR is a product of the European Union as economic union this may seem uncontentious. However, concomitant with particular aims of neoliberal capitalism it is important to note that GDPR specifically aligns economic and social progress with protecting natural persons with regard to the processing of their personal data. Like the technological innovations it aims to regulate (of which we may count blockchain, although as this essay will suggest, the matter is not so straightforward), GDPR fosters the organization of consumption which presupposes, as Bernard Stiegler argues, 'that the becoming of *social systems* must *structurally submit* to the becoming of the *economic system*' (Bernard Stiegler, *For a New Critique of Political Economy*. 2010. Cambridge: Polity, p.82)

motivations driving the development of legislative mechanisms such as GDPR and a variety of blockchain data management applications. Underlying the arguments made here, therefore, is the claim that is necessary to *follow the desire* of stakeholders in order for regulators to understand the nature of control and data sovereignty, as well as what is powering the engine of the nascent blockchain moment in which data sovereignty is finding prominence.

2 THE RISE OF DATA DYSPHORIA

Cyberspace, as a shared dimension but unequal community, is in a moment of unease over the ways and means of data creation, dissemination and preservation, including methods of storage on- and offline. Communication and circulation of commercial and personal data increasingly occurs amid threats of intermeddling and exposure to varieties of exploitation. This unease has manifested itself in recent months in scandals involving the 'psychological profiling' of personal data in the course of supposed civic and democratic processes. The company Cambridge Analytica, whose 'data harvesting' practices and psychographic analyses of user content from sources such as Facebook led to accusations of dubious interventions in and effects on the US Presidential elections and UK European Union Referendum [3]. Facebook's Mark Zuckerberg's subsequent tour of apology, confession and defiance in front of US government and European Commission representatives in early 2018 amid accusations that the company 'weaponised' personal data only served to add intrigue and consternation to the prevailing climate of unease[4].

[3] Olivia Solon and Oliver Laughland, "Cambridge Analytica closing after Facebook data harvesting scandal", *The Guardian*, 2 May 2018. https://www.theguardian.com/uk-news/2018/may/02/cambridge-analytica-closing-down-after-facebook-row-reports-say (accessed 4 June 2018)

[4] Carole Cadwalladr and Emma Graham-Harrison, "Zuckerberg set up fraudulent scheme to 'weaponise' data, court case alleges", *The Guardian*, 24 May 2018. https://www.theguardian.com/technology/2018/may/24/mark-zuckerberg-set-up-fraudulent-scheme-weaponise-data-facebook-court-case-alleges (accessed 4 June 2018)

The fall-out from these high-profile and rather salacious examples is a type of user/subject unease that I refer to as *data dysphoria*, which involves but also transcends specific examples of dubious commercial data practice and pervades cyberspace. In conjunction with this unease there have emerged ideas and mechanisms to 'take (back) control' of one's personal data that provoke the desire for meaningful practices of data self-care in the subject, but which, I argue, instead entangle the subject in a burgeoning mesh of fantasy in which control and data sovereignty are always possible but never attainable[5]. Hence the extent to which data subjects are actually capable of or willing to assume control of personal data in a fully informed way is entirely unclear. Use of a banking app on a smart phone to manage one's finances is convenient, for example, but it does not require the user to negotiate the intricacies of global finance. On the contrary, the convenience of banking apps masks the extent to which personal finance (the credit held in a current or savings account) is embedded in a vast complex of different financial products and networks over which the user has little insight and no meaningful control. Banking apps, therefore, represent a negligible and *de minimis* form of user control, not a radical mode of individual financial liberation. This model is articulated by a wide range of contemporary data management platforms, mechanisms and applications, all of which are directly or indirectly hungry for data[6].

Data dysphoria and its corresponding structure in fantasy describe part of the conscious and unconscious negotiations subjects make with networks, systems and the increasing levels of computational autonomy and authority that are in every sense alien and

[5] Whether or not the inclusion of "back" in the notion of "taking control" is relevant here is debateable. Personal data is not a new phenomenon, it predates modern systems of networked computation. But the control sought arguably transcends the type or form of data and speaks to a more profound sense of individualized self-care. In which case, today's data subjects are not invested in taking *back* control of personal data, by, for instance, returning to old paper records or index cards (forms that were arguably less amenable to transparency anyhow and therefore not desirable by contemporary standards), but only taking control as a progressive standard within broader concerns for self-care.

[6] See, for example: Nick Srnicek, *Platform Capitalism*. 2017. Cambridge: Polity

radically unknowable to the vast majority of users caught by and within them[7]. Importantly, as a symptomology, data dysphoria and fantasies of control also describe affects not online but in the 'real world'. Cyberspace (including databases, networks, systems, or interfaces) in this case does not "solve" the "problems" *qua* messiness inherent in human endeavour (as long, that is, as the primary role of cyberspace is to serve humanity), but represents ever expanding frontiers into which human psychology inevitably moves, may flourish but, equally, falters.

Data dysphoria has, I suggest, particular resonance in terms of the relationship between, what GDPR calls, data subjects, controllers and handlers[8]. In particular how these categorisations and the regulations more broadly sit within a discourse of data sovereignty ('taking control'), which at first blush implies empowerment of the data subject but risks, I argue, satisfying ideals of consumer protectionism above all else. That is, supporting the sovereignty of data subjects insofar as they remain efficient, engaged economic subjects within the ambit of neoliberal capitalism; subjects who without demur bear a financial cost for taking part in history, by investing all their energy into creating new "free" markets and ensuring all social life is calibrated to the logic of those markets[9]. The irony being that the self-care insisted upon by data subjects who are "sovereign" assumes nothing more a form of control that is contingent upon the constraints placed on the subject by neoliberal capitalism, and therefore is not a form of control the data subject

---

[7] As James Bridle maintains: 'If we do not understand how complex technologies function how systems of technologies interconnect, and how systems of systems interact, then we are powerless within them, and their potential is more easily captured by selfish elites and inhuman corporations' (James Bridle, *New Dark Age: Technology and the End of the Future*. 2018. London: Verso, pp.2-3)

[8] https://www.eugdpr.org/the-regulation.html (accessed 6 June 2018)

[9] Adam Greenfield makes a similar point but specifically targeted at the role Ethereum, the organization behind the other major public blockchain alongside the Bitcoin blockchain, is having on shaping individual adaption to and adoption of blockchain applications such as smart contracts and tokens (i.e. Ether) allowing for participation in decentralized autonomous organizations (DAOs). See: Adam Greenfield, *Radical Technologies: The Design of Everyday Life.* 2018. London: Verso

is free to exercise or enjoy at all[10]. To paraphrase Jodi Dean, taking control in this instance does not delineate data subjects from a *rest of us* 'whose work, lives, and futures are expropriated, monetized, and speculated on for the financial enjoyment of the few', instead it serves to highlight the actual complicity of those data subjects in sustaining neoliberal capitalism and 'the extent of the class power of an elite that has gotten us to think in terms of competition, efficiency, stock markets, bonuses, and financial success'[11]. 'Taking control' is thus an illusion or, more precisely as this essay will argue, a *fantasy of data sovereignty* constructed by neoliberal capitalism but ultimately maintained by the data subjects caught within it.

GDPR is not the only feature of prevailing data sovereignty models, debates, and corresponding regulatory conundrums of interest here. New networked technologies coming to the fore promise to perform at once a comparable and conflicting role to the legislation in securing personal data. The presence of such technologies instead risk problems for regulators charged with aligning technological capabilities with public interest because they call into question the validity and cogency of the regulatory enterprise and in particular whether regulations can or indeed must bend when to do so would satisfy broader economic and political demands for 'innovation'. Equally problematic however, is the position of individuals (data subjects) seeking a reliable and honest appraisal and means of accountability of data management mechanisms who become caught between narratives of 'stifling' regulations devised by politically accountable bodies (such as GDPR), and 'innovative' applications developed by private enterprise. The networked technology of interest here are distributed ledgers (DLT), or as they are more popularly known *blockchains*, an application layer on the World Wide Web widely known as the infrastructure supporting cryptocurrencies such as Bitcoin, but

[10] See: Robert Herian. *Regulating Blockchain: Critical Perspectives in Law and Technology*. 2018. London: Routledge
[11] Jodi Dean, *The Communist Horizon*. 2012. London: Verso, pp.69-73

which has more recently expanded conceptually to other commercial, non-commercial, and civic fields[12].

3 PARADOX AND CONVERGENCE

GDPR was introduced by the European Union (EU) in May 2018 to replace the 1995 Data Protection Directive (DPD). The regulation represents an extraordinary and in some cases unwelcome reality in the context of cyberspace and blockchain as a continuation of the European Union's 'particularly strong constitutional tradition of privacy protection' and development of EU data protection law[13]. The EU's influence in this regard extends far beyond the boundaries of the Union, which thus implies a far-reaching impact of the GDPR for blockchain use-cases that do not specifically, intentionally or directly involve personal data of EU citizens. 'The EU has successfully influenced other regional privacy laws by restricting the transfer of personal data from member states to countries without adequate privacy protection', Brown and Marsden point out, and this 'determination of "adequacy" overseen by the European Commission, in practice requires other states to introduce most of the key protections [from EU data protection directives and regulations] into their own national laws'[14].

The impact of GDPR remains largely speculative at the time of writing. By definition the regulation is likely to impact a wide range of blockchain use-cases in the EU and beyond. Key questions for the GDPR versus blockchain debate, questions of both paradox and convergence, begin with *control of personal data*, specifically who within the context of a

[12] A wide variety of definitions and descriptions of blockchain exist. Whilst each attaches significance to different applications of the technology, privacy in the case of personal data for example, most share the same key characteristics bundled-up within the following sort of narrative: blockchains are *distributed, immutable, shared (peer-to-peer) ledgers* on *decentralized* networks that provide data and information *privacy, auditability* and *transparency* within systems and institutions and across networks, and enable *accountability* and *trust* between parties to a transaction or exchange who do not know one another.

[13] Ian Brown and Christopher T. Marsden, *Regulating Code: Good Governance and Better Regulation in the Information Age*. 2013. Cambridge: The MIT Press, p. 59

[14] Brown and Marsden, 2013, p.59

blockchain application is controlling data and thus accountable for its administration within the scope of the regulation. 'The tension between the GDPR and these novel decentralized databases [i.e. blockchains] indeed reveals a clash between two normative objectives of supranational law', argues Michèle Finck, 'fundamental rights protection on the one hand, and the promotion of innovation on the other'[15]. Fundamentally GDPR is aimed at facilitating data sovereignty models in commercial and civic life that give back control of personal data to data subjects, and thus puts data controllers and to some extent handlers on notice[16]. The same cannot necessarily be said about blockchain. As Jacek Czarnecki maintains: 'The controller determines the purposes and means of the processing of personal data. Does such an entity exist at all in the context of a distributed blockchain? We can potentially treat transaction-confirming miners as controllers (in the case of the proof-of-work consensus) - something that in the case of large public blockchains will be unfeasible in practice'[17]. Control equally concerns jurisdiction, in terms of the jurisdiction in which a data controlling party (blockchain node or miner for example) is located and thus the possible or extent of the laws governing them. Winston Maxwell and John Salmon also point to the impact upon issues of control wrought by the different varieties of blockchain, namely permissioned, permissionless, and so on[18].

'Blockchain' is not a monolithic description or definition, but covers a heterogeneity of technological features and possibilities. For present purposes we can recognise at least

---

[15] Michèle Finck, "Blockchains and Data Protection in the European Union", *European Data Protection Law Review*, Vol. 4 (2018), Issue 1, p.17

[16] "25 May – GDPR tightens data protection rules for companies and gives people back control". *European Commission*. 2018. https://ec.europa.eu/unitedkingdom/news/25-may-%E2%80%93-gdpr-tightens-data-protection-rules-companies-and-gives-people-back-control_en (accessed 25 May 2018)

[17] Jacek Czarnecki, "Blockchains and Personal Data Protection Regulations Explained". *Coindesk*. 26 April 2017. https://www.coindesk.com/blockchains-personal-data-protection-regulations-explained/ (accessed 20 April 2018)

[18] Winston Maxwell and John Salmon, "A guide to blockchain and data protection". *Hogan Lovells*. September 2017. https://www.hlengage.com/_uploads/downloads/5425GuidetoblockchainV9FORWEB.pdf (accessed 20 April 2018), pp.16-19

three main types of blockchain or ledger: *permissioned*, *permissionless*, and *hybrids*. Permissioned ledgers are not public but operate in closed systems. They provide many of the same features of public (permissionless) ledgers (of which the Bitcoin blockchain is the most obvious examples) including transparency and peer-to-peer transactions, but are deployed within closed networks like an intranet or back-office system. This ensures the ledger is accessible to those with requisite permissions. A permissionless *public* ledger on the other hand, can, in theory, be viewed by anyone at any time because it resides on the network and 'not within a single institution charged with auditing transactions and keeping records'[19]. Hybrids combine permissioned and permissionless ledgers, meaning data from a closed network can be shielded by a registry layer and moved or released to permissionless blockchains for the purposes of allowing public scrutiny of prescribed or specified data at a given point in time[20]. The hybrid distinction also includes the option of using ledgers, most likely in permissioned form, as an *access control* medium for other, additional registries or databases in off-chain or offline servers and storage infrastructures.

The impact of GDPR on concepts and use-cases flowing from the blockchain ecosystem is not negligible, and forthcoming impact assessments will likely be necessary for use-cases relating to permissionless, public blockchains, as well as those for civic service management of sensitive data such as health records[21]. The necessity of impact assessments for private or enterprise blockchain is less clear however, as Andries Van Humbeeck maintains: 'An important aspect of GDPR on blockchain is the fact that personal data is not to leave the EU. This is a major problem with public blockchains, since there is no control on who hosts a node. This is less an issue when it comes

[19] Don Tapscott and Alex Tapscott, *Blockchain Revolution: How the Technology behind Bitcoin is Changing Money, Business and the World*. 2016. London: Portfolio Penguin, p.6
[20] See for example: *Factom: Business Processes Secured by Immutable Audit Trails on the Blockchain*, Version 1.0, 17 November 2014. www.factom.org (accessed 27 February 2018)
[21] Maxwell and Salmon, 2017, p.21

to private or permissioned blockchains'[22]. In this sense the GDPR is arguably already performing a broad-ranging *ex ante* regulatory function that some blockchain stakeholders will view as counterproductive to innovation. But in doing so it is fulfilling, I argue, an important public interest by constraining the imposition of private commercial interests, and preventing those interests from dominating all avenues or channels of data communication and dissemination.

Rights for 'data subjects' under GDPR include: access to personal data and supplementary information, which involves submission of a subject access request (SAR); objections to certain forms of processing including direct marketing and for research and statistics; rectification of inaccurate and incomplete personal data; erasure of personal data, otherwise known as 'the right to be forgotten'; the restriction of processing of personal data; rights relating to profiling and automated decision making, a right that could impinge upon the 'invisible' machine-to-machine capabilities that blockchain is able to facilitate via smart contracts; and claims for compensation for damage caused by a data breach. Further, limitations on transferring data and information outside of the European Union other than for prescribed reasons, places restrictions on the free-flow across geographical and jurisdictional space. Many of the rights and restrictions the GDPR introduces contradict the ways in which existing global computer networks and databases operate, and this includes blockchain. Indeed, as Finck maintains, even before the GDPR came into force it could be considered outdated with respect to blockchain applications because 'it simply cannot account for the technology's characterising features'[23].

---

[22] Andries Van Humbeeck, "The Blockchain-GDPR Paradox". *Medium*. 21 November 2017. https://medium.com/wearetheledger/the-blockchain-gdpr-paradox-fc51e663d047 (accessed 20 April 2018)

[23] Finck, 2018, pp.32-33

Of the new rights under GDPR, two pertinent examples that do not sit comfortably with what for many stakeholders are core and desirable features of blockchain are Article 22 dealing with automated data processing, and Article 17 focusing on the right to be forgotten. In terms of Article 22 the issue can be specifically attributed to blockchain applications such as smart contracts and decentralised autonomous organizations (DAOs), both of which engender a high degree, if not entirely autonomous (machine-to-machine) mode of operation that clearly risks contravening the fundamental rights of the data subject under the Article 'not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her'. Likewise, with regard to Article 17 the core capability of blockchains to maintain data 'immutability' that can create 'transparency' in order to foster 'trust' conflicts with the right of the data subject to have prescribed data erased.

Self-proclaimed blockchain 'czarina' and Forbes Magazine contributor Andrea Tinianow maintains that 'the GDPR gives its EU citizens the "right to be forgotten." EU citizens can demand that organizations remove their PII [the personally identifiable information of EU citizens] from active use so that nobody else can access that information ever again'[24]. It is important to note that 'erasure' is not an absolute right to be forgotten under the terms of the legislation however, and if, for example, the data involves defence of a legal claim or has overriding public interest then a data controller can refuse to comply with the right. 'The goal of GPDR is to "give citizens back the control of their personal data, whilst imposing strict rules on those hosting and 'processing' this data, anywhere in the world', says Van Humbeeck, and 'one of the things GDPR states is that data "should be erasable". Since throwing away your encryption keys is not the same as

[24] Andrea Tinianow, "GDPR Isn't The Answer, But Blockchain Is", *Forbes*. 4 June 2018. https://www.forbes.com/sites/andreatinianow/2018/06/04/gdpr-isnt-the-answer-but-blockchain-is/#75e88f8848bd (accessed 5 June 2018)

'erasure of data', GDPR prohibits us from storing personal data on a blockchain level. Thereby losing the ability to enhance control of your own personal data'[25]. For Van Humbeeck this is the paradox of GDPR and blockchain. Maxwell and Salmon describe the issue further:

> One of the design features of blockchain architecture is that transaction records cannot be changed or deleted after-the-fact. A subsequent transaction can always annul the first transaction, but the first transaction will remain in the chain. The GDPR recognises a right to erasure. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. What constitutes "erasure" is still open to debate. Some data protection authorities have found that irreversible encryption constitutes erasure. In a blockchain environment, erasure is technically impossible because the system is designed to prevent it[26].

The right to be forgotten linked to the erasure of personal data thus strikes at the heart of blockchain's immutability and its overall effectiveness. Following the logic above, once immutability is brought into question or falls completely through general implementation of mechanisms for undoing chains, this brings into question both the creation of transparency and the ability to foster trust. And, some will argue, without the ability to foster trust or at least to do so without the evil necessity of having to rely on institutional middlemen like banks or government, what is the point of blockchain? One answer is either to find parity, convergence and harmony between GDPR provisions and blockchain applications, or, as a more extreme response, for blockchain to supersede GDPR, as Tinianow implies by the title of her article "GDPR Isn't The Answer, But Blockchain Is".

---

[25] Van Humbeeck, 2017
[26] Maxwell and Salmon, 2017, p.15

Moreover Tinianow is quick to raise old and trite accusations of the evils of regulation, namely, that innovators risk drowning in regulations and regulators should therefore back-off, thus creating more space for blockchain 'solutions' to thrive. 'Between the reporting requirements and the destructibility requirements, organizations that dabble in PII *will now be awash in new obligations and massive potential liabilities in the event they fail to comply*' [emphasis added], claims Tinianow, therefore many in 'the blockchain space are exploring how the GDPR and the blockchain can coexist, as the right to erasure appears to conflict with immutability of the information on a blockchain'[27].

For blockchain use-cases to remain viable against the backdrop of GDPR an industry in workarounds exploiting cracks in the detail of the GDPR have been in business since the reality of what the legislation would entail began to emerge in the blockchain ecosystem in early 2017. 'Smart contracts will contain mechanisms governing access rights', claim Maxwell and Salmon, 'therefore the smart contract can be used to revoke all access rights, thereby making the content invisible to others, albeit not erased'[28]. Meanwhile, 'a popular option to get around this problem is a very simple one', says Van Humbeeck, 'you store the personal data off-chain and store the reference to this data, along with a hash of this data and other metadata (like claims and permissions about this data), on the blockchain'[29]. But, as Van Humbeeck also admits, the term 'workaround' is a clear acknowledgement of the regrettable positon the GDPR puts the ecosystem in, and that 'compromise is rarely good for business'[30]. This is an illustration of the point that classic regulatory conundrums turn on the extent to which regulatees are compliant or can made to be compliant in the future. As Stuart Biegel maintains with regard to the Internet but in terms arguably appropriate to the present discussion:

---

[27] Andrea Tinianow, 2018
[28] Maxwell and Salmon, 2017, p.15
[29] Van Humbeeck, 2017
[30] Van Humbeeck, 2017

> Under current conditions, given the highly participatory nature of online activity and the distributed, anarchic design of cyberspace itself, there are a host of ways to get around most restrictions that may be imposed. In addition, new architectural changes can often be countered by other code-based solutions. Thus a proposed regulatory approach may not be possible unless those that have the ability to resist agree to go along with the plan[31].

Impacts from GDPR versus blockchain remain inconclusive. What is obvious already however is the desire some blockchain stakeholders have to exploit, as best they can, uncertainties existing within the four corners of the GDPR using *know-how*, or what Biegel calls 'the ability to resist' that comes from understanding a technology, its capabilities and limitations, better than the regulator. Thus while the regulation is forcing compliance to some extent, it is by no means watertight and concerns for regulators ought to surround greater desires of stakeholders to undermine the regulations rather than comply with them. Test cases in the coming months and years will necessarily interpret the regulation further, and these cases are guaranteed to involve blockchain as long as stakeholders push concepts and use-cases to the limits of compliance.

The alternative for some, of course, is for blockchain to simply replace GDPR because it is capable of performing the same role. 'I consider a different model for protecting the sanctity of our PII, one where individuals control their own digital identities using blockchain technology', says Tinianow, continuing:

> This model, called self-sovereign identity, suggests that individuals control the information related to their existence on this planet, including birth, education, marital status, professional credentials, and medical records. It is all encompassing. Under this regime, individuals give limited access to

[31] Stuart Biegel, *Beyond our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace*. 2003. Cambridge: The MIT Press, p.361

> third parties, and provide only that information that is needed to transact the business at hand, and only for that specific purpose. If individuals were able to take full control of their PII, they would be able to share their most personal information on the most limited basis. Because the record of the access is recorded to the blockchain, just like the GDPR requirements, there would be an immutable record of who was accessing the information and how the information was being used[32].

What Tinianow proposes is nothing new in terms of blockchain concepts. Avenues for the commodification or exploitation of data held on the blockchain are limited, some have long argued, because the technology affords users greater individual control in ways that previous technologies have not. On this account blockchain heralds a paradigm shift in commercial practices relating to big data and its exploitation. Melanie Swan is one who believes blockchain will achieve this end and refers to the technology on this basis as a 'push technology', because it allows user to initiate and *push* 'relevant information to the network', rather than 'pull' technologies that allow user data to be *extracted* and are therefore 'essentially centralized honey-pots'[33]. Whether blockchain will enable a meaningful shift from data harvesting, extraction and exploitation by business to data control by individuals that mirrors long-standing notions of property ownership, namely, the owners prerogative to use, abuse and alienate their data as and when they see fit, is yet to be tested at scale.

A role for commercial business in the provision of platforms and interfaces for managing and auditing data on blockchain on behalf of customers, consumers or clients is, however, more of a given, one that could see and, indeed, arguably is already seeing rapid advances towards data sovereignty models. A move which will mean commercial practices

[32] Andrea Tinianow, 2018
[33] Swan, 2015, p.4

increasingly internalized by individuals *qua* data subjects, something that is capable of providing huge savings for commercial actors in infrastructure costs for example, whilst arguably intensifying an already generalized reliance on markets and providing more potential commercial revenue streams, not less, from 'honey pots' of personal data freely given subjects who are simply fulfilling their obligations within capitalism as engaged economic citizens. Blockchain, I suggest, turbocharges individualism by fully *economizing* all social life. Moreover it fits the narrative of short-term innovation and investment strategies that Bernard Stiegler associates with the problematic of expedient consumerism[34]. '[T]he organization of consumption', Stiegler argues, 'presupposes that the becoming of *social systems* must *structurally submit* to the becoming of the *economic system*, something enabled by granting the latter full control over technological becoming, that is, over the *technical system* – this submission being obtained by capturing and harnessing the attention of consumers, by diverting their libidinal energy toward objects of innovation, and by controlling their behaviour via marketing'[35].

4 FANTASIES OF DATA SOVEREIGNTY

Like GDPR, the broader, mainstream emergence of blockchain technology in the present moment of data dysphoria is no accident: it is part *reaction* to it, and part *exploitation* of it. The technology satisfies, at least in theory, 'problem'/'solution' matrices with deep roots in a wide variety of global economic, political , social, legal and cultural contexts - too many to cover or mention during the course of this essay. 'Solutions' dreamt up by a variety of stakeholders including entrepreneurs, venture capitalists, and technologists who consider blockchain-led socioeconomic and political characteristics of transparency, disintermediation, post-trust, and so on to be the keys to healthier cyber-socialites and ontologies. There are no shortage of businesses promoting the benefits of blockchain-led

[34] Stiegler, 2010, p.83
[35] Stiegler, 2010, p.82

digital economies through idealizations of secure, peer-to-peer, data-as-property paradigms that promise to empower users by allowing them to unlock 'value' from their personal data in the form of 'micropayments' - a model of granular payments that individuals, as well as corporations, can derive from *all* forms of data exploitation large and small. Far from being novel enterprises a number of these business models necessitate conventions in offline and off-chain markets and consumerism models and thus require high levels of interoperability between different interfaces (both *smart* and *dumb*), whilst also sustaining forms of centralization and mediation that correspond closely to the logic of existing patterns of commercial development that blockchain, it was hoped and lest we forget, was meant to destroy.

Once a fully-fledged peer-to-peer digital economy is up and running on blockchain and users are happily transacting personal data therefore, will traditional (capitalist) business models fall away and create a post-capitalist, consumer-led economic society? It may rather be the case, I suggest, that data subjects auto-exploit by relying on data sovereignty mechanisms, models, skills and techniques *given to them* as indisputable *tools of engagement*; a clear contradiction if we take as our definition of sovereignty 'the receiving of a general recognition of exclusive domain and consequent possession of the capacity to establish rules of conduct within a particular field of action'[36]. On this point we see the root of the fantasy of data sovereignty begin to show itself, because the façade of subject/object choice as a condition of contemporary economic engagement is revealed to be mere belief in the organizational networks enveloping the 'free' economic subject as data subject. In other words, it is an illusion that a data subject has 'capacity to establish rules of conduct within a particular field' because 'a general recognition of exclusive

[36] Sarah Manski and Ben Manski, "No Gods, No Masters, No Coders? The Future of Sovereignty in a Blockchain World". *Law & Critique*. 2018. (forthcoming)

domain' has never existed but is instead *always already* capitalism's domain and the data subject a material site for its ideological (re)production[37].

'Self-sovereign identity technology can put the control [of personal data] in the hands of individuals' Tinianow affirms[38]. For control to manifest in the manner Tinianow envisages, however, would involve wholesale transformations of the present model of socioeconomic organization and hegemony, that is, transformation of capitalism into a new state of economic organization that is actually predicated on more not less self-interest - the notion of self-sovereignty is arguably axiomatic and thus doubles-down on the significance placed on self-interest in Tinianow's account. Given the fundamental tenets of capitalist 'free' enterprise include supply and demand and 'winner takes all' market engagements grounded in the necessity of self-interested economic subjects, it is hard to see how more self-interest is going to fundamentally 'disrupt' the prevailing economic model, or, indeed, encourage it towards some specious notion of post-capitalism. This is because, I argue, it is not meant or designed to. Instead it is a fantasy of economic perfectibility by the data subject at work in the model of data or identity self-sovereignty. Capitalism is not seen by Tinianow as a problem to be solved, but rather the architecture supporting blockchain concepts and implementation. Therefore notions of data or identity self-sovereignty derive from capitalist and, capitalism's 'mutant form'[39], neoliberal structures in fantasy that insist on the perfection and wholeness-of-being attainable through economic practice and self-care. Data practice and data self-care emerge as species of broader capitalist practice: a practice of the practice that maintains capitalism's prominence whilst resisting countervailing and critical notions of data sovereignty from within non-market and non-competitive communities on- and offline.

---

[37] Louis Althusser, *On Ideology*. 2008. London: Verso, pp.46-47
[38] Andrea Tinianow, 2018
[39] Byung-Chul Han, *Psycho-Politics: Neoliberalism and New Technologies of Power*. Translated by Erik Butler. 2017. London: Verso, p.5

An example of a stakeholder promoting commercial model of this sort is Sovrin, a non-profit foundation that is nonetheless enmeshed in a web of private enterprise and for-profit interests acting as "stewards" for the foundation's projects[40]. A clear influence on Tinianow's thinking, Sovrin summarize their approach to data sovereignty "problems" as follows:

> Digital identity is one of the oldest and hardest problems on the Internet. There is still no way to use digital credentials to prove our online identity the same way we do in the offline world. This is finally changing. First, the World Wide Web Consortium is standardizing the format of digitally-signed credentials. Secondly, public blockchains can provide decentralized registration and discovery of the public keys needed to verify digital signatures. These two steps pave the way to establish a global public utility for *self-sovereign identity* - lifetime portable digital identity that does not depend on any central authority and can never be taken away. The Sovrin Network has been designed exclusively for this purpose, including governance (the Sovrin Foundation and the Sovrin Trust Framework), scalability (validator and observer nodes and state proofs), and accessibility (minimal cost and maximum availability). Most importantly, Sovrin implements Privacy by Design on a global scale, including pairwise pseudonymous identifiers, peer-to-peer private agents, and selective disclosure of personal data using zero-knowledge proof cryptography. The emergence of this infrastructure can transform at least four major markets: identity and access management, cybersecurity, RegTech, and data integration. To provide economic incentives for credential issuers, owners, and verifiers, the Sovrin protocol will incorporate a digital token designed

[40] See: https://sovrin.org/stewards/ (accessed 5 June 2018)

> expressly for privacy-preserving value exchange. The Sovrin token should enable a global marketplace for digital credentials of all types and value levels together with ancillary markets for digital credential insurance and permissioned first party data (direct from the customer)[41].

Firstly, the reference to portability and Privacy by Design is noteworthy in Sovrin's model for self-sovereign identity precisely because it aligns their blockchain vision with key citizen rights found in GDPR[42]; or rather it offers an alternative monetizable version to it, prompting the question: why settle for GDPR protections when the *prosumer* can instead create markets in order to freely exploit themselves whilst enjoying the GDPR-like protection offered by the technology? Like Tinianow, Sovrin have no interest in disavowing the central place of capitalism in their blockchain model, and they are quick to position markets as the motivating force for 'selective disclosure' of personal data on blockchain. Sovrin's proposal is therefore one directed toward more commercial exploitation not less, only via a different route: the (re)generation and transformation of markets into self-constituted markets in, amongst other things, credentials and identity attribution. For many blockchain stakeholders, Sovrin and Tinianow included, this is precisely the point and promise of blockchain and thus uncontentious; the very definition of control is a data subject realizing their own 'value'. Consumers rather than the bogeymen of 'third parties' can and ought to control the ways and means of exploitation, and thus we should instead be talking about *auto-exploitation* as the positive configuration of blockchain as a techno-social and techno-economic medium.

What is perhaps most astonishing about the blockchain moment has been the ability of stakeholders to convince the world of the desirability of digital ledgers as immaterial

---

[41] The Sovrin Foundation, *Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust, Version 1.0*. January 2018. https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf (accessed 5 June 2018), p.2

[42] https://www.eugdpr.org/the-regulation.html (accessed 6 June 2018)

objects of ritual and devotion. We are witnessing a possible rise of ledger society in which rituals of verification will become more central to the everyday normative functions of society than Michael Power first envisaged two decades ago[43]; where the ledger assumes vast status as a ritual object and multivocal symbol, its referents 'not all of the same logical order' but 'drawn from many domains of social experience and ethical evaluation' for the purposes of allowing data subjects to perform economically[44]. The digital ledger *qua* blockchain is arguably an example of greater transformation of the mundane into the specular than even mobile phones achieved with the inauguration of smart phones. Moreover this explains the fetishistic and feverish churn of blockchain concepts and use-cases and why venture capital is investing increasingly large amounts of money to service the erotics – '*not* the physical mating urge', but rather 'the desire for recognition by others and for wholeness'[45] - of emergent blockchain markets. For example, blockchain-based companies with little more than a concept to their name have been raising eye-watering amounts of capital – estimates as of summer 2017 put the figure of blockchain investment at $4.5 billion and this will certainly be exceeded in 2018[46].

There is undoubtedly something that can be called a trend or fashion occurring around blockchain, whereby entrepreneurs turn to blockchain for a 'solution' with no real need to understand whether it is the best or most effective option for the proposed 'problem', or, indeed, whether there is real 'problem' that blockchain is required to solve in the first place. The excitement surrounding the 'disruptive' potential of blockchain begins not with technology therefore but with fantasies and objects of desire coveted by entrepreneurs,

---

[43] Michael Power, *The Audit Society: Rituals of Verification*. 1997. Oxford: Oxford University Press

[44] Victor Turner, *The Ritual Process: Structure and Anti-Structure*. 1969. New Brunswick: Aldine Transaction, p.52

[45] Jeanne Lorraine Schroeder, *The Triumph of Venus: The Erotics of the Market*. 2004. Berkeley: University of California Press, p.86

[46] Jonathan Ponicano, "Blockchain Tops $4.5 Billion In Private Funding This Year, But Deal Growth Stalls". *Forbes*, 22 September 2017. https://www.forbes.com/sites/jonathanponciano/2017/09/22/blockchain-tops-4-5-billion-in-private-funding-this-year-but-deal-growth-stalls/#1bb344ef74c6 (accessed 27 February 2018)

which is not the same as entrepreneurs 'dreaming big' with the technology - a staple narrative within the confines of the entrepreneurial class. The result is a jumble of misunderstandings as to the precise nature and value of blockchain as a technology, and reductionist narratives of blockchain as a global economic panacea rushing to fill gaps evacuated of critical reason and reinstitute what Herbert Marcuse long ago called the 'comfortable, smooth, reasonable, democratic unfreedom' that 'prevails in advanced industrial civilization, a token of technical progress'[47].

If the first decades of the new millennium have been dominated by the rise of digital socialization built around an Internet of information and experience sharing, and of an expansion in the population of digital subjectivities willing to expose themselves online and coming to know what it means to *engage* and *participate* - albeit falsely, as we are increasingly learning today with scandals over mass data use by companies like Facebook promoting participation of subjects as monetizable data sets - then might blockchain as the economic layer the web has never had signal a retreat from the idea of cyberspace as a phenomenology of socialization to something more plain, more 'boring'[48], but at least honest? An Internet or more specifically application layers including the World Wide Web that are more streamlined and less noisy or a fake participatory may be an attractive proposition in some instances, dominated not by an interest in reposing socially in cyberspace with the fatigue and data dysphoria that increasingly accompanies that obligation. Using technology to simply transact and exchange with more brute efficiency may be attractive if it means less emphasis on marshalling one's efforts and energies to build the sorts of social and trusting relationships that accompany offline and off-chain trade. In other words, a Sovrin-like model of unadorned utilitarianism, a *pure* free-

[47] Herbert Marcuse, *One-Dimension Man: Studies in the ideology of advanced industrial society*. 2002. London: Routledge, p.3

[48] Lana Swartz, "Blockchain Dreams: Imagining techno-economic alternatives after Bitcoin". *Another Economy is Possible*. Edited by Manuel Castells. 2017. Cambridge: Polity Press, pp.82-105

market capitalist vision of cyberspace that blockchain brings to prominence through the incorruptible and bureaucratic simplicity of the ledger-form.

The implications of blockchain fermenting a streamlined and deeper economization of cyberspace, and transforming it into an ever more perfect market, is not something to be welcomed, but lamented I argue. Through such propositions we find an impoverished humanity existing through technology beset by and implicated in the ideals and practices of financial economy first and last. 'Networked communication and information technologies are exquisite media for capturing and reformatting political energies', argues Jodi Dean, they 'turn efforts at political engagement into contributions to the circulation of content, reinforcing the hold of neoliberalism's technological infrastructure'[49]. Where blockchain figures in Dean's analysis is still evolving as the technology moves from the brute economics of cryptocurrencies to more obvious political domains such as the provision of public services and democratic accountability vis-à-vis voting and government transparency initiatives. At heart, however, blockchain projects that usurp the protectionism of GDPR in favour of *prosumer* initiatives enable a vision of humanity caught in endless engagement with practices of transacting and exchanging that do not reflect efficiency or create time able to be spent on meaningful non-economic and non-financialized pursuits, but because transaction and exchange are, under the aegis of capitalism and neoliberalism, ends in themselves to be enjoyed ritually and fetishized. Contemporary ledger technologies and the peer-to-peer networks they support not only enable contributions to the circulation of content, as Dean expresses it, but more accurately economize those contributions in accordance with ever more crystallized, neoliberal ideals. The data subject amid peer-to-peer networks must thus search for and anticipate each new transaction and exchange as a fantasy of data sovereignty: an erotic

[49] Jodi Dean, *Democracy and Other Neoliberal Fantasies: Communicative Capitalism and Left Politics*. 2009. Durham: Duke University Press, p.32

encounter with the *other* of and within the network worthy of sharing the performative demands and conduct of data self-care and neoliberal self-hood.

5 CONCLUSION

As a neoliberal capitalist technology blockchain implants economic reason in the contexts and fields it touches - as the 'the economic layer the Web has never had'[50] - and this applies equally to conditions for the creation of data sovereignty. This means a technology *always already* skewed in favour of economic interests *qua* neoliberal capitalist ideology that both places the technology and its effects ahead of public interest and political accountability and works in order to erode them. To some extent it can be argued that GDPR, in contrast to blockchain projects such as Sovrin, recognises this by constraining elements of contemporary free-economic practice such as aggressive data handling and methods of exploitation, including auto- or self-exploitation. But the control GDPR and blockchain alike promise is, as this essay has argued, contentious if not fantastical. Moreover a paradox, perhaps a vicious circle, exists in desires to usurp GDPR in favour of a technology (blockchain) seen as capable of solving the problems wrought by contemporary techno-sociality and the obligations it enforces upon data subjects to become data sovereign.

The significance of blockchain stems at present from its status as a sublime digital artefact *qua* fantastical cultural product, not because of any actual economic or political force that the technology has yet brought to bear on- or offline. Blockchain's material impact can largely be attributed to the ways in which stakeholders talk about it (hype, rhetoric, marketing, and so on), rather than from any serious applied influence the technology has, as yet, had. But this is changing, and the example of Sovrin is symptomatic of the change occurring. Jodi Dean describes how the 'technological fetish

[50] Melanie Swan, *Blockchain: Blueprint for a New Economy*. 2015. Sebastopol: O'Reilly, p.vii

covers and sustains a lack on the part of the subject. It protects the fantasy of an active, engaged subject by acting in the subject's stead […] enabling us to go about the rest of our lives relieved of the guilt that we might not be doing our part and secure in the belief that we are, after all, informed, engaged citizens'[51]. Moreover a 'technological fetish is at work when one disavows the lack or antagonism rupturing (yet producing) the social by advocating a particular technological fix', claims Dean, the '"fix" [the 'solution'] lets us think that all we need is to extend a particular technology and then we will have a democratic or reconciled democratic order'[52].

Blockchain, or rather its applications, whilst fulfilling the fetishistic role in fantasy Dean professes, arguably has nothing to do with or no interest in reconciliation of the democratic order in terms of data sovereignty, an appeal to the political that contemporary visions of blockchain saturated as they are in economic reason undermine and undo. Instead fantasies of data sovereignty and the linkage to data dysphoria, are symptomatic of the insistence of a capitalist and neoliberal techno-sociality that 'informed, engaged citizens' must translocate into single embodiments and digitalized economic avatars: data subject, controller and handler as an ontological singularity who's unwavering belief belongs to and on the blockchain.

[51] Dean, 2009, pp.37-38
[52] Dean, 2009, p.38