THE UNIVERSITY of EDINBURGH

Edinburgh Research Explorer

The alegality of blockchain technology

Citation for published version:
De Filippi, P, Mannan, M & Reijers, W 2022, 'The alegality of blockchain technology', *Policy and Society*, vol. 41, no. 3, pp. 358-372. https://doi.org/10.1093/polsoc/puac006

Digital Object Identifier (DOI):
10.1093/polsoc/puac006

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Publisher's PDF, also known as Version of record

Published In:
Policy and Society

General rights
Copyright for the publications made accessible via the Edinburgh Research Explorer is retained by the author(s) and / or other copyright owners and it is a condition of accessing these publications that users recognise and abide by the legal requirements associated with these rights.

Take down policy
The University of Edinburgh has made every reasonable effort to ensure that Edinburgh Research Explorer content complies with UK legislation. If you believe that the public display of this file breaches copyright please contact openaccess@ed.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 24. Mar. 2025

Policy and Society, 2022, **41(3)**, 358–372
DOI: https://doi.org/10.1093/polsoc/puac006
Advance access publication date 16 February 2022
Original Research Article

The alegality of blockchain technology

Primavera De Filippi[1,2], Morshed Mannan[3,4] and Wessel Reijers[5,6,7]

[1]Chargée de recherche, CERSA | CNRS, Paris, France
[2]Faculty Associate, Berkman Klein Center for Internet & Society, Harvard University, Cambridge MA, USA
[3]Max Weber Fellow, Robert Schuman Centre for Advanced Studies, European University Institute, Florence, Italy
[4]ICDE Research Affiliate, The New School, NY, USA
[5]Postdoctoral Researcher, University of Vienna, Vienna, Austria
[6]Visiting Fellow, Robert Schuman Centre for Advanced Studies, European University Institute, Florence, Italy
[7]Visiting Scholar, Technion, Haifa, Israel
Corresponding author: Wessel Reijers, Camillo-Sitte-Gasse 9/29; 1150 Wien. Email: wessel.reijers@univie.ac.at

Abstract

Similar to the early days of the Internet, today, the effectiveness and applicability of legal regulations are being challenged by the advent of blockchain technology. Yet, unlike the Internet, which has evolved into an increasingly centralized system that was largely brought within the reach of the law, blockchain technology still resists regulation and is thus described by some as being "*alegal*", i.e., situated beyond the boundaries of existing legal orders and, therefore, challenging them. This article investigates whether blockchain technology can indeed be qualified as alegal and the extent to which such technology can be brought back within the boundaries of a legal order by means of targeted policies. First, the article explores the features of blockchain-based systems, which make them hard to regulate, mainly due to their approach to disintermediation. Second, drawing from the notion of alegality in legal philosophy, the article analyzes how blockchain technology enables acts that transgress the temporal, spatial, material, and subjective boundaries of the law, thereby introducing the notion of "*alegality by design*"—as the design of a technological artifact can provide affordances for alegality. Third, the article discusses how the law could respond to the alegality of blockchain technology through innovative policies encouraging the use of regulatory sandboxes to test for the "functional equivalence" and "regulatory equivalence" of the practices and processes implemented by blockchain initiatives.

Keywords: decentralized autonomous organizations; alegality; legal theory; blockchain governance; regulatory sandbox

Blockchain technology poses challenges to policymakers and regulators, mostly due to the decentralized nature of public, permissionless blockchain-based networks. The operations of these networks are determined by a computer protocol enforced by a decentralized network of nodes responsible for processing transactions and recording them into the blockchain (Nakamoto, 2008). To the extent that all network nodes follow the same protocol, no single party can unilaterally dictate or influence the operations of the network. Moreover, because of its decentralized nature, even if one or more of these nodes were forced to shut down the network (due to a technical glitch or regulatory constraint), it could continue to operate as long as there remains at least one running node (Swan, 2015). Public

© The Author(s) 2022. Published by Oxford University Press.
This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial License (https://creativecommons.org/licenses/by-nc/4.0/), which permits non-commercial re-use, distribution, and reproduction in any medium, provided the original work is properly cited. For commercial re-use, please contact journals.permissions@oup.com

Downloaded from https://academic.oup.com/policyandsociety/article/41/3/358/6529327 by guest on 07 November 2024

blockchains are also essentially pseudonymous in the sense that anyone can join and operate the network without having to disclose their real identity (Lai & Chuen, 2018). They only need a public–private key pair to generate a public address and interact with the network. It can, therefore, be challenging for governments or other centralized authorities to impose their sovereignty over these blockchain-based networks due to their limited ability to identify network actors or control the network's operations. On the whole, blockchain-based systems exhibit a set of distinctive characteristics—namely related to (a) decentralization, (b) transnationality, (c) tamper-resistance, (d) pseudonymity, (e) lack of coercion, (f) trustlessness, and (g) operational autonomy—which, combined, make them particularly resistant to legal regulation (De Filippi & Wright, 2018).

Because of these distinctive characteristics, blockchain technologies can be said to challenge the *boundaries* of the legal order(s) in which they operate. This means, amongst other things, that these legal orders are *unable to see* certain activities conducted through blockchain-based networks or simply that they *lack the codes* to understand or even just describe them. Influential proponents of blockchain technology such as Gavin Wood (2014) have asserted that blockchain technologies are potentially "alegal," to the extent that they support and enable activities that are neither legal or illegal nor extralegal. However, whatever the accuracy of this claim might be, it has never been assessed within the broader theoretical framework of alegality in legal philosophy. This paper will critically connect the different discourses of alegality using the characterization of alegality in legal philosophy to assess the claim to alegality of blockchain technologies. It first investigates the extent to which blockchain technology can indeed be considered as alegal, to subsequently explore new paths for governmental authorities to regulate blockchain technology, despite its alegal characteristics.

The contributions of this article are threefold. First, the article contributes to the existing academic discourse on governance and regulation *by* the infrastructure while exploring the notion of blockchain as a regulatory technology that operates within its own technical framework and independently of existing regulatory frameworks. By linking this discourse with the relevant academic literature on alegality, the article investigates the reasons why blockchain technologies can be said to operate outside of the purview of the law and how existing legal orders could potentially respond to that challenge. Second, the article also contributes to the literature on alegality by introducing the notion of *alegality by design*. Thus far, the academic discourse on alegality has mainly focused on alegal acts such as speech acts performed by human beings, with little attention paid to the politics of technological artifacts themselves (Winner, 1980). Indeed, if the potential for alegality is embedded into the technological architectures through which people interact, the technological design of a blockchain-based system can be regarded as providing the affordances for an alegal act. Third, assessing the alegal nature of blockchain technology makes it possible to suggest specific policy recommendations on how blockchain technology may be regulated. In this regard, we propose expanding the use of regulatory sandboxes.

The section "Defining Alegality" of this article outlines the concept of alegality and the different ways in which this multifaceted idea has been defined and understood both by the academic literature and by practitioners in the blockchain space. The section "Alegality of Blockchain Technology" illustrates the alleged alegal nature of blockchain technologies through a variety of examples, including the publication of the Bitcoin whitepaper, TheDAO attack, the pseudonymity inherent in public blockchain networks, and the characteristics of smart contracts. The section "Policies for Blockchain Governance" shows that the claim that blockchain technologies can promote alegal activities does not mean that these activities can never be regulated or brought within the ambit of the law. It concludes by offering a policy path to address the alegal characteristics of blockchain through the use of regulatory sandboxes to test for the "functional equivalence" and "regulatory equivalence" of the practices and processes implemented by blockchain technology.

Defining alegality

The distinctive features of blockchain-based systems have led key stakeholders in the blockchain space to describe public, permissionless blockchains as "alegal" systems. This term was introduced in the blockchain space by Ethereum co-founder Gavin Wood (2014) to advance the idea that decentralized blockchain-based systems are similar to forces of nature (Lustig, 2019): they are neither legal nor illegal; they merely subsist outside of the legal realm. The claim made by these commentators is not that blockchain-based platforms are difficult to regulate (as the argument was with regard to the Internet in its early days) but rather that they should be regarded as neither an object nor a subject of law (Atzori,

Downloaded from https://academic.oup.com/policyandsociety/article/41/3/358/6529327 by guest on 07 November 2024

2015). Indeed, to the extent that they do not depend on a single centrally controlled web interface and no physical assets are involved in any of the associated transactions, these platforms can be designed to largely ignore the coercion of the law (Miller, 2019): not only do they not depend on the coercive force of the State to enforce transactions and commitments but they are also indifferent about the legal context in which transactions and commitments occur.

To explore whether blockchain-based systems can indeed be claimed to be alegal, we first examine what meanings have thus far been ascribed to the concept of alegality with reference to more general examples. Alegality provides a conceptual basis to perceive and understand all that exists beyond the law, all that lies beyond the distinction of legality and illegality created by the State's legal apparatus (i.e., the legislature, courts, and tribunals). In other words, alegality encompasses all the acts that, at a given moment, exceed the intelligibility of the law and cannot be reduced to the legal/illegal binary. They present a particular form of distinctiveness—or "strangeness" (Lindahl, 2013b, 730)—that makes them difficult to identify or categorize within the scope of legal orders. As such, alegality can broadly be understood as the "capacity to be neither legal or illegal, the ability to exist and act in the interstices, or perhaps beyond or outside, the dominant modes of [..]legal production" (Hamzić, 2017, p. 191).

It has to be noted that, although we connect the claims to alegality made by blockchain proponents with the broader academic literature on alegality, we do not intend to establish a basic similarity between these two different usages of the term. Indeed, as we shall see, the definition of alegality proposed by blockchain advocates and that provided by academic scholars lie far apart. Yet, we argue that, even if they think differently about the origin of this phenomenon, both share a common intuition concerning the emergence of specific acts that fall beyond the boundaries of the legal order and might thus require it to evolve in order to accommodate these acts. While Lindahl identifies alegal acts as those that do not properly fit into the established legal/illegal categories of a legal order because of their "strangeness" (Lindahl, 2013b), Wood (2014) seems to assume that technological systems (e.g., those powered by blockchain technology) can also present alegal challenges because of their strangeness or "inhumanity" (Hui, 2019).

A widely accepted definition of a legal order is as an "aggregate of […] general and individual norms that govern human behavior" (Kelsen & Paulson, 1982, p. 64), which is typically, but not always, created through legislative acts. These legislative acts are underwritten by the coercive powers and apparatus of the State (Pistor, 2019). They are the basis for public and private law, which also underpin transactional ordering through the establishment of property rights and binding commitments between private parties. Hans Lindahl, one of the main theorists on the topic of alegality, broadens this definition whilst contemplating emergent global legal orders. His definition is particularly relevant when considering blockchain technologies. He contends that legal orders are a particular type of collective action: *"institutionalised* and *authoritatively mediated* collective action" (Lindahl, 2018, p. 60) [emphasis added]. By this, he means that a legal order relies on specific authorities that regulate collective action on behalf of all participants through the articulation, monitoring, and upholding of (capaciously defined) rules. Moreover, unlike some other forms of collective action, a legal order can create impersonal or anonymous relations between participants and with the authorities in charge of defining and applying the rules. This means that, for there to be a legal order, most of the participants have to agree to be subject to a common set of rules (what Lindahl more capaciously calls a "default setting") and accept the role of institutions as authorities responsible for the institutionalized mediation and application of these rules. This requires accepting the existence and validity of these common rules as a consequence of the authority held by certain offices (e.g., the office of the US President), regardless of the particular individual that holds that office at any given point in time (Lindahl, 2018, pp. 54–59; Shapiro, 2014, p. 286).

Specifically, Lindahl (2013a) argues that all legal orders determine *who* ought to do *what*, *where*, *and when* through the setting of boundaries—both tangible and intangible—which stipulate what is legal and what is illegal. These dimensions correspond to the "spheres of validity" of the norms in a legal order (Lindahl, 2018, p. 51). As such, legal orders are always and necessarily bounded: not only are they circumscribed by the set of legal provisions that constitute the legal system, each of these provisions also exhibits a particular set of *boundaries* that establish a distinction between the legal and the illegal (Lindahl, 2010, 35). Lindahl categorizes these boundaries into four broad categories: (a) *temporal*, (b) *spatial*, (c) *material*, and (d) *subjective* boundaries, discussed in more detail below. According to Lindahl, an alegal act is one that fundamentally questions or challenges these boundaries, thereby revealing the

Downloaded from https://academic.oup.com/policyandsociety/article/41/3/358/6529327 by guest on 07 November 2024

boundary as a limit and potentially triggering a change of the legal order (Lindahl, 2009, p. 57, 2018, p. 65). Importantly, the opening toward another possible form of legality through the commission of alegal acts is central in distinguishing alegality from illegality—which is not concerned with alternative legalities but rather with reinforcing existing legal boundaries. We delineate below the four types of boundaries identified by Lindahl, which we interpret in light of the existing literature on alegality.

First, legal orders are *temporally* bounded: laws are created at a particular point in time and, in principle, should not be retroactively applied to previous events. In doing so, laws provide an orientation of when something is permitted or ought to be done—and when it is not (Lindahl, 2013a, pp. 20–21). Most importantly, laws are stipulated based on past acts and knowledge about past behaviors; they cannot cover all the unprecedented acts and unknown unknowns that lie in the future. Thus, paradigmatic examples of alegal acts that transgress the *temporal* boundaries of a legal order are those acts that initiate something new, those that aim to establish a new form of legality that is incommensurable with the existing one. The commission of such an alegal act would thereby usher in a novel way to structure the sequence of when and how something can be appropriately done. These acts can range from foundational acts seeking to constitute a new legal order when the distinction between legal and illegal is formed (e.g., the declaration of an independent state by revolutionaries) to official acts in which the sovereign decides on the existence of a state of exception and suspends some of the established distinctions between legality and illegality for a limited period of time (e.g., suspension of rights of assembly during a national emergency).

Second, legal orders are *spatially* bounded: they operate within particular territories in which rules of legality and illegality apply—even though these territories may sometimes overlap. While these boundaries may be the territorial boundaries of a state, they also include novel spatial configurations–such as multinational corporations with operations spanning across multiple jurisdictions—whose internal legal order transcends state territorial boundaries (Lindahl, 2018, pp. 143–144). In Lindahl's view, even a transnational space like cyberspace is ultimately affected by the spatial boundaries of the law. He uses the example of the B2C e-commerce platform eBay to argue that even if user agreements and online dispute resolution mechanisms are used to decouple national law from private "eBay law," at least two physical places are interconnected into a spatial unity for the purpose of payment and goods shipment: the seller-place and the buyer-place (Lindahl, 2018, p. 152). Alegal acts that transgress the spatial boundaries of an established legal system are those that put into question the physical places where certain actions are permitted or ought to take place. The border crossing of immigrants is an example of such an act, as each crossing questions the distinction between legality and illegality drawn by the polity which immigrants are trying to enter. According to Lindahl, the entry of impoverished economic migrants into the EU and their employment in the internal market underlines the possibility of an *alternate legality*—one where the "illegal" participation of these migrants in the internal market would be possibly "legal," and the restrictions on a global free movement of labor would be regarded as "illegal" (Lindahl, 2008, p. 126).[1]

Third, legal orders are *materially* bounded: they are expressed through definite configurations of rights and obligations, which, combined, determine the variety and content of the acts that can be done at any point in time and place (Lindahl, 2013a, p. 21). Alegal acts can transgress the *material* boundaries of a legal order by doing things that have not been (expressly) authorized or permitted, with a view to reconfigure that specific set of rights and obligations that stipulates what ought to be done in a particular legal order. An example is that of peoples' tribunals which are formed to deliberate and rule on a particular dispute (e.g., Permanent Peoples' Tribunal on Myanmar) that emerged as a response to the limitations of the international criminal justice system in investigating international crimes and alleged perpetrators. These tribunals take on a quasi-institutional form and adopt languages, processes, and symbols of State tribunals, but rely on alternative conceptions of justice (e.g., reconciliation) and differing modes of court procedure (e.g., more relaxed conceptions of legal standing), and are not supported nor expressly recognized by established legal orders. Their decisions have no binding force, but they are instead framed as a response to institutional failure and thereby exemplify and promote an alternative, better system. For Hughes (2019, pp. 473–475), it is these very characteristics that make these people's tribunal not illegal but alegal.

[1] Lindahl (2008, p. 126) claimed that all four boundaries of a legal order were transgressed by border crossings, but, here, we focus on the spatial dimension.

Downloaded from https://academic.oup.com/policyandsociety/article/41/3/358/6529327 by guest on 07 November 2024

Fourth, legal orders exhibit *subjective* boundaries that determine whose acts are to be either legally protected or sanctioned. Most legal orders implement different tiers of subjecthood, in which one's legal status (conferred by, e.g., citizenship) allows for varying degrees of rights and protections. Asylum seekers or prisoners are archetypal examples of legal subjects whose status may entitle them to some rights and protections but exclude them from others (e.g., voting in national elections). Alegal acts that transgress subjective boundaries are generally those where a subject challenges the prohibitions on their conduct that arise due to their particular status, with the intention of reconstituting the boundaries of this prohibition elsewhere, such as, for instance, slaves who participated in the abolitionist movement in the US. In extreme cases, legal orders may also cast subjects outside of their boundaries even with no geographical displacement, for instance, in the case of the Roman *Homo Sacer* (Agamben, 1998), the condemned individual who is placed beyond the law through a legal verdict, no longer benefiting from legal protection and thus becoming legitimately killable by anyone.

Alegal acts may transgress multiple boundaries at the same time. Inner-city slums in countries like Brazil and Pakistan have been described as alegal spaces (Hamzić, 2017, p. 199). While not being entirely free from the state apparatus, residents in these localities resist the imposition of state law and largely self-regulate, thereby transgressing spatial boundaries (i.e., of a city's legal order), material boundaries (i.e., enabling or restraining what residents can do, which do not exist elsewhere) and subjective boundaries (i.e., enabling or restraining acts by virtue of their position as poor citizens and migrants). In these contexts, as De Sousa Santos (1977, p. 5) argues, the incapacity of the state legal system to affect or effectively regulate these activities leads to the creation of an "internal legality, parallel to—and sometimes conflicting with—state legality, a kind of popular justice."

Importantly, alegality should not be confused with extra-legality. Extra-legality refers to acts that are explicitly exempted from legal scrutiny by a legal order and hence—paradoxically—fall within its boundaries. An example would be the immunities from criminal prosecution granted to diplomats when performing official acts in the legitimate exercise of their functions (Shi, 2021, p. 46). Another example is the corporate charter given to corporations in the 18th century that granted them "legal exemptions to benefit public welfare" (Barkan, 2013, p. 16) that protected them from acts of the sovereign. In contrast, alegality exists at the interstices of the law and extends beyond it, with its "infinite possibilities" continuing to exist even after the boundary between legal and illegal has been redrawn by a sovereign power (Shimabuku, 2019, p. 1–2).

The transgressive potential of alegal acts remains latent but ever-present. When these acts manifest, they have the potential to affect or reshape the existing boundaries of an established legal order. In Lindahl's terms, at the juncture where these transgressive behaviors and actions manifest, the boundaries that unite the legal order can be experienced as *limits* to what lies beyond (2013a, 41). In his view, these limits, which include and integrate certain ought-places (i.e., who ought to do what, where, and when) and exclude others, are a fundamental feature of any legal order (Lindahl, 2019, p. 5). It is often in response to alegal acts that these boundaries may be reordered by a legislative or judicial power so as to reframe the boundaries of (il)legality and the "limit between collective self and other-than-self" (Lindahl, 2019, p. 18).

However, there are some situations in which alegal acts, although transgressive to the legal order, cannot easily be resolved through a legal reform. In such cases, the boundaries of the legal order can be regarded as *fault lines*, whereby the normative claims raised by the alegal acts cannot be addressed by the legal system, without putting into jeopardy the very identity of that system (Lindahl, 2013a, pp. 3–4, p. 165, 2019, p. 22). If a legal order is viewed as a "*closed, self-referring* and *autopoietic* system that creates, amends, interprets and justifies itself through itself" (Kedar, 2006, p. 101) [emphasis added], fault lines reveal the frailties of this view. In addressing *fault lines*, a justification also has to be sought from beyond the seemingly closed, self-referring legal order (e.g., in politics) to decide on whether its identity should be placed in jeopardy or not. But, as the normative point of the existing legal order is threatened and the alegal acts are irreducible to this legal order, an opening is created to a different normative conceptualization of how legal and illegal is distinguished (Schaap, 2009, p. 4). Tuori adds that alegal challenges can also be presented by parallel legal orders, such as indigenous legal systems and state territorial legal systems, with competing normative claims about how legal/illegal should be distinguished (Tuori, 2016, p. 134).

In view of the above, three *types* of alegal acts can be distinguished. First, there are common, everyday acts that are situated beyond the boundaries of the law in a practical sense. These are all these acts

Downloaded from https://academic.oup.com/policyandsociety/article/41/3/358/6529327 by guest on 07 November 2024

that are not intended to be covered by liberal legal systems, such as the act of thinking. Second, there are acts that are not yet intelligible to the legal order but that can be. This includes both acts that were potentially meant to be covered by the law but were not properly encompassed, as well as those that were deliberately excluded but have now become relevant for legal regulation. This could be due to a shift in circumstances or the advent of new technologies. This is the case, for instance, of all these acts enabled by the advent of the Internet and digital technologies, which required a legal reform in order to restore the previous equilibrium of the law (e.g., extending copyright law to fight online piracy), or which triggered the establishment of new legal rules in order to cover a new usage of technology (e.g., autonomous vehicles). Third, there are specific alegal acts that could possibly be brought within the boundaries of the legal order, although doing so would be challenging to the extent that it would require a significant reform of the legal system as a whole, in that the mere absorption of these acts within the legal system would potentially create an incongruence or inconsistency with the other provisions of the legal order. These acts enable us to identify the *fault lines* of a legal system and are of particular interest to us in our analysis of the alegality of blockchain technology.

In what follows, we expand on Lindahl's conceptualization of alegal acts as political acts in order to investigate how blockchain technology, by virtue of its *technological design*, could be said to generate specific affordances for alegal action. The reasons to expand Lindahl's conception of alegality are twofold: on the one hand, Lindahl omits to discuss the political stance of technological artifacts, which could be intentionally designed to support or facilitate alegal acts; on the other hand, Lindahl exclude from the notion of political acts the possibility of a technologically mediated political act, thereby failing to acknowledge the alegal affordances that blockchain technology can have.

First, even though Lindahl (2013a, 2013b, 2018) engages with the discussion of (a)legality in cyberspace, he does not thematize the role of technology as such. He draws extensively from systems theory to set up his account of cyberlaw, but, in doing so, he adopts an instrumental understanding of technology linked to cybernetics. That is, Lindahl regards technology as a neutral instrument in the unfolding of collective action that leads to an institutionalization of the legal order. This comes to the fore in Lindahl's discussion of a confrontation of claims mediated by cyberspace, between people like Barlow (1996), who proclaims the independence of the cyberspace as a separate legal order, and the Somali man who attacked the Danish cartoonist Westegaard in his home for drawing a provocative religious cartoon and publishing it online, who challenges the idea that state law does not have the ability to reach the cyberspace (Lindahl, 2013b). In his account, the technological medium through which these claims are made seems of almost no consequence; the same argument would hold if controversial cartoons would not have been published online but rather in a paper magazine. Digital mediation is just regarded as a new way by which people can relate to other people and things in the world (Lindahl, 2018, pp. 150–151); it does not transform these relations. Yet, philosophers of technology have convincingly argued that technologies enshrine political values (Winner, 1980) and that the technical medium through which actions are conducted inform those very actions (Latour, 1994). Hence, the possibilities afforded by Internet technologies enable new technological practices that might supplant the law with its own legal order (hence, the argument that "code is law"), but at the same time might trigger a legal reform to accommodate these new practices (e.g., a new understanding of the "right to be forgotten"). Similarly, the technological design of blockchain technology—as a decentralized, transnational, and autonomous infrastructure—enables the emergence of a new autonomous legal order (so-called *lex cryptographica*), which can also present alegal challenges to the extent that it might destabilize the boundaries of existing legal orders. We refer to this as *alegality by design*.

Second, the notion of technologically mediated alegal action is largely omitted by Lindahl because alegality, in his view, exclusively refers to the comportment of an agent who engages in political action. Lindahl builds his conceptualization of alegal action upon Arendt's notion of political action, which she describes as "acting and speaking in concert [..] in the space of appearance" (Arendt, 1958, p. 181; Hans Lindahl, 2006). Specifically, in Arendt (1958), we do not readily find the possibility of technological practice as political action since political action, for Arendt, is never an act of making or fabricating, but only one of direct communication.[2] However, if—as we argue above—artifacts "have" politics

[2] In setting out the ontology of the *Vita Activa*, Arendt claims that technologically mediated activities would be the activities of *homo faber*, belonging to the realm of "work," not political action. Yet, within Arendt's oeuvre, there is the unexplored possibility of hybridity, of what might be named "work in the mode of action" (Reijers, 2020). Such an activity aims at creating a durable world (a built environment with institutions) while at the same time being open to the plurality of human action.

Downloaded from https://academic.oup.com/policyandsociety/article/41/3/358/6529327 by guest on 07 November 2024

(Winner, 1980), it becomes necessary to expand the notion of political action (as envisioned by Lindhal and Arendt) to also encompass a subset of technological mediated actions. As such, alegality can also be enacted through specific practices of design, use, and appropriation of technologies. We argue that such an understanding of political action is necessary in order to account for the distinctive characteristics of blockchain technology and the affordances that they provide to alegal acts. Accordingly, the design, use, and appropriation of these technologies can be regarded as political activities in and of themselves, which can—in specific circumstances—also qualify as alegal acts.

Alegality of blockchain technology

We can investigate the alegality of blockchain-based systems by considering the extent to which they enable acts that transgress the boundaries of the legal orders in which they operate. We analyze in particular the manner in which blockchain technology may reveal the fault lines of established legal orders. This will be shown by considering how extending the boundaries of the law in order to bring the alegal acts enacted by blockchain technology back within the scope of the traditional legal/illegal dichotomy could potentially disrupt the legal system as a whole by introducing a series of incompatibilities or inconsistencies within the legal order.

With the publication of the Bitcoin whitepaper, Satoshi Nakamoto carried on a foundational act that brought into being a new monetary system that did not exist before and could, therefore, not be encompassed by the law. The deployment of Bitcoin can be seen as a transgressive act within established financial legal orders as it questions the core role of trusted financial intermediaries with an alternative peer-to-peer network that can function as an effective monetary system and which relies on confidence rather than trust (De Filippi et al., 2020). As such, Bitcoin challenges the distinction between legality and illegality in the context of monetary and financial regulations by creating a new monetary system that could potentially undermine the exclusive roles of legally established financial institutions (De Filippi & Mauro, 2014), most notably with regard to the issuance and recognition of money as legal tender. If central banks have a legal monopoly over the production and supply of legal tender, the publication of the Bitcoin whitepaper has the potential to challenge this monopoly. It presents an opening to *"another legality"* (Lindahl, 2009, p. 60), one where Bitcoin could potentially be recognized as legal tender by a sovereign nation, even if it is not issued by any central bank. As such, the publication of the Bitcoin whitepaper reveals a *temporal fault line* in the legal order: could Bitcoin be recognized as legal tender when it is not backed or issued by any sovereign authority? In the Western political imagination, the issuance of coinage has long been seen to be the prerogative of the sovereign, second only to the monopoly on legitimate violence and the making of laws (Bodin & Franklin, 1992, 78; Woodhouse, 2017). Recognition of Bitcoin as legal tender would require the legal order to reconstitute its boundaries to forego the expectation that legal tender can only be issued or backed by sovereign states. Despite the associated administrative, legal, and political implications that such an act might entail, such a reconstitution has recently occured in El Salvador (Associated Press, 2021)—the first country to recognize Bitcoin as legal tender.

The advent of Bitcoin, and blockchain technology, more generally, also resulted in the development of new applications that can more easily escape the force of existing regulations (De Filippi, 2014). These applications leverage the pseudonymity of Bitcoin or other cryptocurrencies to facilitate money laundering, create decentralized marketplaces for illicit goods or services (Trautman, 2014), and provide a new payout mechanism for cyberattacks. The tamper-resistant features of blockchain technology can be abused to permanently record questionable content and preclude the exercise of specific rights that require the deletion of content (De Filippi, 2016), such as the right to be forgotten (Finck et al., 2019). These applications are strictly speaking *illegal* in that they are expressly sanctionable by a particular body of law. Yet, the fact that they are illegal in a particular domain does not prevent them from also being *alegal* in another domain to the extent that they can trigger the boundaries or reveal the fault lines of a particular body of law.

These dynamics are particularly visible in the context of property law. Traditional property rights are defined by the law and can, therefore, also be taken away by the law. Hence, someone who stole or fraudulently acquired possession of a particular piece of property could be found to lack legal ownership of the property and have it frozen or seized by law enforcement authorities. The advent of blockchain technology, however, enabled the emergence of new "crypto-assets"—like cryptocurrencies or blockchain tokens—that do not follow the same rules. Blockchain technologies rely on a new

Downloaded from https://academic.oup.com/policyandsociety/article/41/3/358/6529327 by guest on 07 November 2024

technologically driven paradigm for ownership that does not necessarily map onto legal ownership: anyone holding the private key associated with a particular Bitcoin wallet will be *technically* the owner of any Bitcoins within that wallet, even if he or she would not qualify as the legal owner thereof.

Interim injunctions and worldwide freezing orders may be imposed on intermediaries like cryptocurrency exchanges and crypto-custodians in an effort to enforce legal ownership.[3] Yet, for all those who do not rely on third-party intermediary services, no enforcement authority will have the ability to unilaterally seize their Bitcoins, even if they were found guilty to have illegitimately acquired them. Moreover, the pseudonymity and global distribution of people making transactions on a blockchain make it particularly difficult for regulators to identify the actors who should be subject to legal orders and sanctions in the event of a transaction that is deemed to be illegal (Dimitropoulos, 2020, p. 1182). This might, ultimately, create a discrepancy between the legal order and the technical order of blockchain-based applications, whose alternative regime of property rights (involving both pseudonymous parties and algorithmic entities or smart contracts) can thus be said to challenge both the *material* and *subjective* boundaries of the law. The alegality of this alternative property regime has been partially addressed by states' legal order through the Know Your Customer (KYC) requirements imposed on many cryptocurrency exchanges and other custodian wallet operators. However, there remains a particular fault line that is more difficult to address, related to the newfound possibility for algorithmic entities (e.g., smart contracts) to effectively (i.e., technically) own digital assets (both licit and illicit). Reconstituting the boundaries of the legal order to encompass such a regime would require recognition of artificial entities being able to own digital assets, even without any human in the loop.

A striking example of a situation where the distinction between alegal and illegal acts became material in the context of blockchain governance was TheDAO attack. TheDAO was a decentralized investment fund deployed as a smart contract on the Ethereum blockchain in 2016 that raised USD $150 million dollars in 1 month. The peculiarity of this investment fund was that there was no centralized authority in charge of administering the funds; it was collectively managed by the investors themselves (Kaal, 2017). Each investor could participate in the fund's governance in proportion to the amount of funds they each had contributed. Whether people wanted to contribute more money into the fund, propose a particular investment, or vote on the projects that they would like TheDAO to invest in, every interaction had to be done—strictly and exclusively—via a smart contract transaction on the Ethereum blockchain (DuPont, 2019). However, a vulnerability was found in the code of the smart contract governing TheDAO, which was exploited in order to drain the equivalent of over USD $60 million dollars from the fund (Mehar et al., 2019; Santos & Kostakis, 2018). This raised a heated debate within the Ethereum community as to whether this action qualified as theft—in that the draining of funds was counter to the original intentions of the parties and amounted to an illegitimate expropriation of their assets—or whether it could instead be regarded as a legitimate act—in that it did not actually infringe upon the (unintentionally flawed) provisions of the smart contract code (Zhao et al., 2017): *the code is the law*.

Given that the issue has not been brought to court, one can only speculate as to how it would have been decided by a judge. Yet, even if the judge had found that such an action qualified as theft and that the stolen funds should therefore be returned to TheDAO, such a decision could hardly have been enforced. Indeed, TheDAO was not a registered company in any jurisdiction but rather subsisted as a decentralized software entity, replicated on the computer of all network nodes participating in maintaining the Ethereum blockchain. As such, TheDAO was both everywhere and nowhere—ultimately challenging the *spatial boundaries* of the legal order, which typically address enforcement through private international law principles that seek to subject an entity to a particular territory. Even in comparison to the eBay example mentioned above, which could not entirely escape from being rooted in physical places, TheDAO was untethered from any physical location due to the lack of any centralized operator registered in a particular jurisdiction, the pseudonymity of (most of) its participants, the autonomy of the transaction system, as well as the absence of physical goods being transacted. Through its mere existence, TheDAO thus revealed a specific fault line in the existing legal order. Indeed, as a general rule, and in the vast majority of jurisdictions, in order to acquire legal personality, companies or corporations must be registered or recognized by the laws of at least one jurisdiction. Such a territorial approach precludes the legal order from encompassing aspects of transnational unregistered

[3] AA v Persons Unknown & Ors, Re Bitcoin [2019] EWHC 3556 (Comm) (13 December 2019), at [61]; Vorotyntseva v Money-Ltd (T/A Nebus.com) [2018] 9 EWHC 2596 (Ch), at [13].

Downloaded from https://academic.oup.com/policyandsociety/article/41/3/358/6529327 by guest on 07 November 2024

organizations, such as DAOs, which do not have a presence in, or strong ties to, any specific national jurisdiction yet tries to create an equivalent to legal personality and capacity through technological design. While the legal order could potentially expand its scope in order to assign legal personalities to these DAOs,[4] the mere fact of recognizing that such entities are not (necessarily) created by national law would challenge some of the basic axioms according to which artificial legal entities are presently regulated, requiring a radical reconstitution of the spatial boundaries of the law that would entail significant administrative, legal and political changes across multiple legal orders. This is where the fault line arises.

Moreover, because of the characteristics of the Ethereum blockchain, the contentious transaction of TheDAO attack could not be reversed as easily as it could have been in the traditional financial system (Wenker, 2014). The autonomy and immutability of the blockchain code make it impossible for any third-party authority to unilaterally seize stolen digital assets (Raskin, 2014). Thus, the traditional legal system offered limited recourse, as the lack of a centralized authority combined with the pseudonymity of participants made it virtually impossible for the original token holders to reclaim their loss through traditional legal means (Kiviat, 2015). This further reinforces the idea that TheDAO provided an opening to *another legality*: its transnational nature, its technologically driven regime of property rights, and the pseudonymity of most of its participants enabled TheDAO to transgress and effectively operate beyond the *spatial*, *material*, and *subjective* boundaries of the law.

Given the impossibility for any centralized authority to reverse the contentious transaction and restore the original balance of TheDAO, the only way to remedy this problem was for the whole Ethereum network to take a coordinated action and change the protocol of the underlying blockchain so as to retrieve the allegedly stolen funds. Following heated community discussions and opinion gathering, the selected solution was to transfer the balance of the smart contract account where the stolen funds were stored to a new smart contract account, which had been specifically designed to allow for TheDAO investors to withdraw their funds. A significant majority of participating nodes agreed to update their software to reflect the "forking" decision (Voshmgir, 2017), but some did not (Mehar et al., 2019).

This shows how, despite its allegedly *alegal* character, TheDAO was not immune from external intervention. Indeed, while no legal proceedings would have been successful in restoring TheDAO's balance, a collective community intervention ultimately succeeded in retrieving the funds. As such, TheDAO attack—and, in particular, its aftermath—can be assimilated to a "state of exception" that challenged the legal order of Ethereum's internal governance structure (Reijers et al., 2021). Deciding to hard fork was, in a sense, an *alegal* act in and of itself, testing both the *temporal* and *material* boundaries of the internal legal order established by the Ethereum blockchain network. Here, the temporal boundary of the Ethereum blockchain (which is reflected in the principles of temporality and non-retroactive modification of past transactions) was transformed into a fault line, as resolving the case required either reinforcing the existing code-is-law approach (thereby accepting a loss of USD $60 million) or accepting new approach to blockchain governance that recognizes the legitimacy of external interventions, in exceptional circumstances, to reverse or invalidate recorded, yet undesirable transactions. In material terms, the modification of the underlying blockchain protocol constituted a material fault line, in that it undermined the fundamental claim to immutability as regards the protocol or code of existing blockchain-based systems (although not doing so would support acts that some considered to be unjust or even illegal).

Such a coordinated action was ultimately the result of a collective political decision to retrieve the allegedly stolen funds. Although there is no "sovereign" on the Ethereum network, the coordinated action of all network nodes could successfully modify the network protocol (Reijers et al., 2021). Thus, even in the most *alegal* spaces—in *xenotopias* (Lindahl, 2018, p. 29, 65)—governance continues to have an important role to play.

Policies for blockchain governance

Policymakers can respond to the alegal characteristics of blockchain technology in one of two ways: either by extending the scope of existing legal provisions in order to encompass new activities that should be covered by the law or by reducing the law's scope in order to exclude activities that should not

[4] For one example of such an initiative, see COALA, DAO Model Law (2021), available at https://coala.global/wp-content/uploads/2021/06/DAO-Model-Law.pdf.

Downloaded from https://academic.oup.com/policyandsociety/article/41/3/358/6529327 by guest on 07 November 2024

have been encompassed in the first place. In the first approach, policymakers may decide to tackle the alegality of blockchain technology by bringing some of the activities necessary for ensuring the proper operation or maintenance of a blockchain-based network within the scope of the law. Alternatively, in the second approach, they may decide to deliberately exclude certain activities from the scope of the legal order by providing legal immunities allowing for these activities to take place without the usual constraints of the legal system. This explicit exclusion of activities from the traditional legal order would amount to making the *alegal* into the *extralegal*.

Despite their resistance to inclusion within a legal order, *alegal* acts are not entirely immune to the legal system. Indeed, the aftermath of the TheDAO attack provided a clear demonstration that blockchain-based platforms do not exist in a vacuum (De Filippi, 2018); they subsist within a larger ecosystem, and their operations depend on the actions of a variety of actors with divergent or competing interests (Böhme et al., 2015), which are themselves subject to the law.

Accordingly, even if the traditional means of regulation are not readily applicable to some of the operations of a blockchain, there are other ways in which intervention remains, nonetheless, possible (De Filippi & Wright, 2018). Potential means of intervention include, *inter alia*, regulating intermediaries, commercial operators, or mining pools and establishing arbitration systems between governments and cryptocommunities (Dimitropoulos, 2020, 1191). Regulators and policymakers may attempt to impose responsibilities or liabilities onto these actors. This has previously been the approach with regulating the Internet as a global network. Rather than trying to directly regulate the behaviors of Internet users, governments sought to instead regulate strategic gateways and chokepoints, such as Internet service providers. While these approaches to regulation have not yet gained much traction in the blockchain policy arena, the identification of new mechanisms to control or influence the operations of a blockchain-based system will become increasingly necessary (Koens & Poll, 2018), as the technology gets adopted in the context of private companies, public sector agencies or other institutional frameworks (Sulkowski, 2019). An important question to address—as Johnson and Post (1996, p. 1375) had already observed with respect to cyberspace—is who can legitimately exercise control or influence a public and permissionless blockchain network? Relatedly, how can this be done so that the network retains its distributed nature?

It is widely acknowledged today that centralized cryptocurrency exchanges and custodian wallet providers have an important role to play in blockchain governance due to the fact that they act as intermediary operators for all of their users, many of whom will automatically follow any decisions the intermediary takes (with regard to, e.g., choosing one fork over the other). As these intermediaries typically have a presence in a jurisdiction due to licensing requirements, they are also particularly vulnerable to governmental pressures in the countries they operate in. In the US and Europe, cryptocurrency exchanges are required to comply with KYC and Anti-Money Laundering regulations, and some governments may promote the "black-listing" of specific addresses to prevent transactions with persons who have been involved in criminal activities. Such approaches, while effective in addressing specific policy concerns, have the (undesirable) effect of reducing the decentralizing potential of the networks by reinforcing the power and influence of intermediaries.

The contention of Walch (2019) that developers contributing to the code of public blockchain networks like Bitcoin hold fiduciary duties (by default) toward users or third-party operators relying on these networks is also untenable. First, it imposes a duty when open-source software developers have generally enjoyed exemptions from liability for the software they produce, subject to the necessary warranty disclaimers being made (Dixon, 2004). Second, it misunderstands how blockchain networks operate. These developers, unlike centralized platform operators, cannot impose changes onto a network and rely on the active participation and cooperation of network participants to modifications and upgrades (Haque et al., 2019). The same is true for the other types of actors involved in the governance of a blockchain network—be they cryptocurrency holders, miners, validators, commercial operators, influencers, etc. (De Filippi & McMullen, 2018). Hence, while it is legitimate to hold specific third parties accountable for their own actions (e.g., for extortion), it would be problematic and unjust to hold individual actors responsible for actions collectively undertaken by network participants, which they do not single-handedly control.

In some instances where there is alleged criminal or civil liability arising from an act, the State may take the practical step of pursuing those persons who are within their jurisdiction–even if their individual responsibility is marginal. The fear of potential liability may act as a deterrent for persons who reside

Downloaded from https://academic.oup.com/policyandsociety/article/41/3/358/6529327 by guest on 07 November 2024

in particularly litigious jurisdictions from engaging in blockchain governance (Zetzsche et al., 2018). Paradoxically, a state's ability to influence blockchain governance may become more circumscribed as a result of these practices since those who participate in the governance of a blockchain-based system will try to reside and operate outside their jurisdiction.

These suggested approaches to influence the operations of blockchain-based systems are limited in that they do not properly account for the alegal characteristics of these systems. They merely replicate the approach adopted in the context of Internet governance, focusing on those players who can be more easily regulated. These approaches reinforce the boundaries of the legal order through the enactment of draconian regulations rather than exploring the possibility of reconstituting these boundaries in light of the alegality of new technological developments.

Given the specificities of blockchain technology, whose governance involves a multiplicity of actors and interconnected layers, it might be useful to consider alternative means of intervention for policymakers to contribute to improving the governance of blockchain-based systems while being mindful of their distinctive properties and characteristics. Any policy proposal must account for the alegal features of public, permissionless blockchains (such as the impossibility for any one jurisdiction to shut down the entire network), as well as the potential implications of every policy choice, including its ability to alter the collective identity of the legal order. As Lindahl reminds us, alegal challenges that cannot be accommodated into a legal order will not disappear even with the most adroit policy prescriptions (Lindahl, 2019, p. 23). Indeed, his overarching suggestion is that when casting the boundaries of a legal order, one should always acknowledge that there will always be a persistent and unorderable outside that legal order (Lindahl, 2019, p. 28).

Instead of undertaking extensive legal reforms to regulate these blockchain-based systems in an all-encompassing way, which might require either a radical reformulation of the legal order or an actual modification of the underlying infrastructure and political structure of these systems, we propose that policies leverage the notions of *functional equivalence* and *regulatory equivalence* as an alternative means of bringing these systems within the scope of the legal order. *Functional equivalence* relies on analyzing the function of a particular artifact (e.g., paper document) with a view to determining how those functions could be fulfilled through another type of artifact (e.g., electronic document) within a particular legal context (e.g., contract law). Functional equivalence is thus an efficient way to address the *alegality* of the second type—i.e., all these acts that are not yet intelligible to the law, but that easily could be intelligible because expanding the boundaries of the law in order to bring them into scope would not change much of the content nor fundamentally challenge the identity of the legal order. Indeed, the concept of functional equivalence has already been adopted by certain laws, such as the UNCITRAL Model Law for Electronic Commerce which establishes functional equivalence between a paper-based document and an electronic document for the purpose of contracting. *Regulatory equivalence* goes one step further by analyzing the purpose of a particular legal or regulatory provision (e.g., auditing for the purpose of verifying credit-worthiness) to determine under which conditions the same purpose could be achieved, in a wholly different manner, through alternative technological means (e.g., using fully collateralized smart contracts to eliminate counterparty-risk). Regulatory equivalence is also relevant in the alegality context because it allows for objects or activities that are outside of the legal order to be incorporated within it, to the extent that they contribute to supporting an equivalent objective or purpose as some of the legal provisions of the legal order.

To assess whether new usages of blockchain technology can comply with existing regulatory requirements (functional equivalence) or provide equivalent types of safeguards/guarantees to promote existing policy objectives (regulatory equivalence), policymakers around the world should more widely encourage the creation of "regulatory sandboxes." Regulatory sandboxes are mechanisms, often used in the financial industry, to establish a controlled environment for early-stage firms to experiment with new technologies or business models while benefiting from temporary exemptions from existing financial regulations (e.g., unsophisticated investor protection) and legal requirements (e.g., customer protection) within that environment. The term "regulatory sandbox" was coined in 2015 by the Financial Conduct Authority in the UK to describe the environment in which there is an opportunity to develop "mutual learning about the impact of current regulation on new financial products and, more generally, in order to reduce the phase of 'time to market' in financial innovation" (Mangano, 2018, p. 728).

Downloaded from https://academic.oup.com/policyandsociety/article/41/3/358/6529327 by guest on 07 November 2024

A few projects building blockchain-based systems have already gone through regulatory sandboxes in the UK[5] and elsewhere.

To understand how regulatory sandboxes can be useful for establishing functional and regulatory equivalence, consider the example of Initial Coin Offerings. The costs and regulatory burdens of complying with securities regulations are often high enough to dissuade many projects from even trying. Yet, well-designed technological solutions could ensure transparency and contribute to substantially reducing the risk of investors,[6] potentially justifying the establishment of a more lenient regulatory regime for all these initiatives that were to adopt these solutions (Collomb et al., 2019).

The benefit of relying on regulatory sandboxes is that they enable regulators and policymakers to delegate the task of coming up with innovative solutions concerning the regulation of blockchain technology to the actors directly involved in the use of that technology (and who have a better understanding of its respective challenges and opportunities). Over time, if policymakers were to recognize these blockchain-based solutions as either functionally or regulatorily equivalent to the purpose of existing legal provisions, the granting of regulatory exemptions could be implemented outside of the regulatory sandbox, thereby reducing the burden of legal and regulatory compliance to all these actors who would integrate these solutions into their own information system. If successful, this approach would thus support the establishment of novel blockchain-based solutions that *voluntarily* comply with existing policy and regulations, in order to benefit from these regulatory exemptions, without unduly sacrificing the decentralized nature of these systems.

This is—in the words of Agamben (1998, p. 7, 22)—a response to alegality that relies on the notion of *inclusion by exclusion*: by deliberately covering certain activities through legal exemptions, the legal order is simultaneously expanding its scope to encompass these activities and committing to not interfering with these activities, provided that they remain within the scope of the exemption. We acknowledge that this approach, which creates greater room for a nascent private legal order for blockchain-based systems (*lex cryptographica*) will come with its own limits and boundaries in the sense that this private legal order will still have an inside and an (unordered) outside. Accordingly, lex cryptographica will have to face its own set of alegal challenges that stalks every "emergent global legal order like its shadow" (Lindahl, 2019, p. 32). Instead, we see our recommendations as enabling policymakers to navigate the various fault lines revealed by the operation of blockchain-based systems in a manner that is consistent with policy objectives and regulatory requirements while preserving the distinctive properties and accommodating the alegal characteristics of these systems.

Conclusion

Blockchain networks present distinctive characteristics that distinguish them from traditional centralized online platforms. In particular, the inherent resilience, incorruptibility, tamper-resistance, and operational autonomy of blockchain-based systems have led some people to describe them as *alegal*—in the sense that they are neither legal nor illegal, they operate outside of the reach of the law and resist inclusion into a legal order. While the notion of *alegality* has usually been used to refer to specific actions or activities performed by humans, this article also argues that *alegality* can be used to refer to specific technological artifacts, whose inherent characteristics facilitate new types of alegal acts. By introducing the notion of "alegality by design," this paper has shown that the technological design of many blockchain-based systems can support and promote alegal acts through technological affordances. Yet, such a qualification does not relegate these systems to alegality by virtue of them being unregulatable "forces of nature"—as originally claimed by Wood (2014). Rather, blockchain networks and the systems that govern them are *human, all too human*, subject to the social norms and economic imperatives that originate from particular modes of social life.

The proposed policy approach of encouraging the use of regulatory sandboxes opens a fresh set of research questions: what are some of the technological solutions that can comply with existing

[5] For example, the sixth cohort of the UK Financial Conduct Authority's regulatory sandbox had businesses using blockchain for SME invoice financing, tracing donations, and issuing security tokens; https://www.fca.org.uk/firms/regulatory-sandbox/regulatory-sandbox-cohort-6. In Singapore, crypto-custodian firms have also graduated from the Monetary Authority of Singapore's regulatory sandbox; https://www.mas.gov.sg/development/fintech/sandbox (both accessed 28 December 2021).

[6] For example, if all transactions are executed on a public blockchain, one cannot claim to have undertaken a transaction that does not appear on the blockchain or, conversely, to not have engaged in a transaction that does appear on the blockchain. This could go toward replacing expensive reporting obligations.

Downloaded from https://academic.oup.com/policyandsociety/article/41/3/358/6529327 by guest on 07 November 2024

regulatory requirements or provide equivalent types of safeguards/guarantees to promote existing policy objectives? What are the legal and socio-economic limitations of using regulatory sandboxes (Ranchordás, 2021), particularly in the context of blockchain governance? These are some of the questions that need to be explored in future research.

Funding

This research is funded by the European Research Council under the European Union's Horizon 2020 Research and Innovation Programme (Grant Agreement No. 865856).

Conflict of interest

None declared.

References

Agamben, G. (1998). *Homo sacer: Sovereign power and bare life*. Stanford University Press.

Arendt, H. (1958). *The human condition* 24. University of Chicago Press.

Associated Press. (2021, June 9). El Salvador becomes first nation to bitcoin legal tender. *The New York Times*. https://www.nytimes.com./2021/06/09/world/americas/salvador-bitcoin.html.

Atzori, M. (2015). Blockchain technology and decentralized governance: Is the state still necessary? Available at SSRN 2709713. https://dx.doi.org/10.2139/ssrn.2709713.

Barkan, J. (2013). *Corporate sovereignty: Law and government under capitalism*. University of Minnesota Press.

Barlow, J. (1996). *A declaration of the independence of cyberspace*, https://www.eff.org/cyberspace-independence.

Bodin, J., & Franklin, J. H. (Ed.). (1992). *Bodin: On sovereignty*. Cambridge University Press.

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives*, *29*(2), 213–238. https://doi.org/10.1257/jep.29.2.213.

Collomb, A., De Filippi, P., & Klara, S. (2019). Blockchain technology and financial regulation: A principle-based approach to the regulation of ICOs (December 5, 2019). *European Journal of Risk Regulation*, *10*(2), 263–314. https://doi.org/10.1017/err.2019.41.

De Filippi, P. (2014). Bitcoin: A regulatory nightmare to a libertarian dream. *Internet Policy Review*, *3*(2), 1–11. https://doi.org/10.14763/2014.2.286.

De Filippi, P. (2016). The interplay between decentralization and privacy: The case of blockchain technologies. *Journal of Peer Production*, *7*, 0–18. https://ssrn.com/abstract=2852689.

De Filippi, P. (2018, February 28). No blockchain is an Island, in CoinDesk.

De Filippi, P., Mannan, M., & Reijers, W. (2020). Blockchain as a confidence machine: The problem of trust and challenges of governance. *Technology in Society*, *62*, 101284. https://www.coindesk.com/markets/2018/02/28/no-blockchain-is-an-island/.

De Filippi, P., & Mauro, R. (2014). Ethereum: The decentralised platform that might displace today's institutions. *Internet Policy Review*, *25*. https://doi.org/10.1016/j.techsoc.2020.101284.

De Filippi, P., & McMullen, G. (2018). *Governance of blockchain systems: Governance of and by the infrastructure*. COALA & Blockchain Research Institute Big Idea Whitepaper. https://policyreview.info/articles/news/ethereum-decentralised-platform-might-displace-todays-institutions/318.

De Filippi, P., & Wright, A. (2018). *Blockchain and the law: The rule of code*. Harvard University Press. https://hal.archives-ouvertes.fr/hal-02046787/document.

De Sousa Santos, B. (1977). The law of the oppressed: The construction and reproduction of legality in Pasargada. *Law & Society Review*, *12*(1), 5–126. https://doi.org/3053321.

Dimitropoulos, G. (2020). The law of blockchain. *Washington Law Review*, 95(3), 1117–1192. https://digitalcommons.law.uw.edu/wlr/vol95/iss3/3.

Dixon, R. (2004). *Open source software law*. Artech House.

DuPont, Q. (2019). *Cryptocurrencies and blockchains*. John Wiley & Sons.

Finck, M. (2019). Blockchains and the right to be forgotten. In N. Aggarwal, H. Eidenmüller, L. Enriques, J. Payne, & K. van Zwieten (Eds.), *Autonomous systems and the law* (pp. 87–90). C.H. Beck and Nomos.

Hamzić, V. (2017). Alegality: Outside and beyond the legal logic of late capitalism. In H. Brabazon (Ed.), *Neoliberal legality: Understanding the role of law in the neoliberal project* (pp. 190–209). Routledge.

Haque, R., Seira, R., Plummer, B., & Rosario, N. (2019). *Blockchain development and fiduciary duty*. Stanford Journal of Blockchain Law & Policy, *2*(2), 139–187. https://dx.doi.org/10.2139/ssrn.3338270.

Downloaded from https://academic.oup.com/policyandsociety/article/41/3/358/6529327 by guest on 07 November 2024

Hughes, C. (2019). Action between the legal and the illegal: A-legality as a political–legal strategy. *Social & Legal Studies*, *28*(4), 470–492. https://doi.org/10.1177%2F0964663918791009.
Hui, Y. (2019). *Recursivity and Contingency*. Rowman & Littlefield Publishers.
Johnson, D. R., & Post, D. (1996). Law and borders—The rise of law in cyberspace. *Stanford Law Review*, *48*(5), 1367–1402. https://doi.org/1229390.
Kaal, W. A. (2017). Blockchain innovation for private investment funds. U of St. Thomas (Minnesota) Legal Studies Research Paper No. 17–21. https://dx.doi.org/10.2139/ssrn.2998033.
Kedar, N. (2006). The political origins of the modern legal paradoxes. In O. Perez & G. Teubner (Eds.), *Paradoxes and inconsistencies in the law* (pp. 101–117). Hart Publishing.
Kelsen, H., & Paulson, S. L. (1982). The concept of the legal order. *The American Journal of Jurisprudence*, *27*(1), 64–84. https://doi.org/10.1093/ajj/27.1.64.
Kiviat, T. I. (2015). Beyond bitcoin: Issues in regulating blockchain tranactions. *Duke Law Journal*, *65*(3), 569–608. https://scholarship.law.duke.edu/dlj/vol65/iss3/4.
Koens, T., & Poll, E. (2018). The drivers behind blockchain adoption: The rationality of irrational choices. In European Conference on Parallel Processing (pp. 535–546). Springer, Cham.
Lai, R., & Chuen, D. L. K. (2018). Blockchain–from public to private. In D.L. Kuo & R. Deng (Eds.), *Handbook of blockchain, digital finance, and inclusion* (Vol. 2, pp. 145–177). Academic Press.
Latour, B. (1994). On technical mediation - Philosophy, sociology, genealogy. *Common Knowledge*, *3*(2), 29–64.
Lindahl, H. (2006). Give and take: Arendt and the nomos of political community. *Philosophy & Social Criticism*, *32*(7), 881–901. https://doi.org/10.1177%2F0191453706066979.
Lindahl, H. (2008). Border crossings by immigrants: Legality, illegality, and alegality. *Res Publica*, *14*(2), 117–135. https://doi.org/10.1007/s11158-008-9051-5.
Lindahl, H. (2009). The opening: Alegality and political agonism. In A. Schaap (Ed.), *Law and agonistic politics* (pp. 57–70). Ashgate Publishing Limited.
Lindahl, H. (2010). A-Legality: Postnationalism and the Question of Legal Boundaries. *The Modern Law Review*, *73*(1), 30–56.
Lindahl, H. (2013a). *A-legality*. Oxford University Press.
Lindahl, H. (2013b). We and cyberlaw: The spatial unity of constitutional orders. *Indiana Journal of Global Legal Studies*, *20*(2), 697–730. https://www.repository.law.indiana.edu/ijgls/vol20/iss2/7.
Lindahl, H. (2018). *Authority and the globalisation of inclusion and exclusion*. Cambridge University Press.
Lindahl, H. (2019). Inside and outside global law. *Sydney Law Review*, *41*(1), 1–34. http://www5.austlii.edu.au/au/journals/SydLawRw/2019/1.html.
Lustig, C. (2019). Intersecting imaginaries: Visions of decentralized autonomous systems. Proceedings of the ACM on Human-Computer Interaction, 3(CSCW), pp. 1–27. https://doi.org/10.1145/3359312.
Mangano, R. (2018). Blockchain securities, insolvency law and the sandbox approach. *European Business Organization Law Review*, *19*(4), 715–735. https://doi.org/10.1007/s40804-018-0123-5.
Mehar, M. I., Shier, C. L., Giambattista, A., Gong, E., Fletcher, G., Sanayhie, R., Kim, H. M., & Laskowski, M. (2019). Understanding a revolutionary and flawed grand experiment in blockchain: The DAO attack. *Journal of Cases on Information Technology (JCIT)*, *21*(1), 19–32. https://www.igi-global.com/article/understanding-a-revolutionary-and-flawed-grand-experiment-in-blockchain/216950.
Miller, R. (2019). Continuing challenges to international law and order from evolving technologies such as blockchain. *Hirao School of Management Review*, 9, 41–52.
Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. https://bitcoin.org/en/bitcoin-paper.
Pistor, K. (2019). *The code of capital: How the law creates wealth and inequality*. Princeton University Press.
Ranchordás, S. (2021). Experimental regulations and regulatory -sandboxes – Law without order? *Law & Method*, 2021 (December), 1–23. https://doi.org/10.5553/REM/.000064.
Raskin, M. I. (2014). Realm of the coin: Bitcoin and civil procedure. *Fordham Journal of Corporate & Financial Law*, *20*(4), 969–1011. https://ir.lawnet.fordham.edu/jcfl/vol20/iss4/3.
Reijers, W., Wuisman, I., Mannan, M., De Filippi, P., Wray, C., Rae-Looi, V., Vélez, A. C., & Orgad, L. (2021). Now the code runs itself: On-Chain and Off-Chain Governance of Blockchain Technologies. *Topoi*, 40, 821–831. https://doi.org/10.1007/s11245-018-9626-5.
Reijers, W. (2020). Responsible innovation between virtue and governance: Revisiting arendt's notion of work as action. *Journal of Responsible Innovation*, *7*(3), 471–489. https://doi.org/10.1080/23299460.2020.1806524.

Downloaded from https://academic.oup.com/policyandsociety/article/41/3/358/6529327 by guest on 07 November 2024

Santos, F., & Kostakis, V. (2018). The DAO: A million dollar lesson in blockchain governance. School of Business and Governance, Ragnar Nurkse Department of Innovation and Governance. https://digikogu.taltech.ee/et/item/9a66d3af-25ca-4552-8a6d-de54d357ff58.

Schaap, A. (2009). Introduction. In A. Schaap (Ed.), *Law and agonistic politics* (pp. 1–13). Ashgate Publishing Limited.

Shapiro, S. (2014). Massively shared agency. In M. Vargas & G. Yaffe (Eds.), *Rational and social agency: The philosophy of Michael Bratman* (pp. 257–292). Oxford University Press.

Shi, X. (2021). Diplomatic immunity ratione materiae, immunity ratione materiae of state officials, and state immunity: A comparative analysis. *Leiden Journal of International Law*, 34(1), 45–65. https://doi.org/10.1017/S0922156520000606.

Shimabuku, A. M. (2019). *Alegal: Biopolitics and the unintelligibility of Okinawan life*. Fordham University Press.

Sulkowski, A. J. (2019). Blockchain, Business Supply Chains, Sustainability, and Law: The Future of Governance, Legal Frameworks, and Lawyers? Delaware. *Journal of Corporate Law*, 43(2), 303–345. https://djcl.org/portfolio/volume-40-2-2-2.

Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc.

Trautman, L. J. (2014). Virtual currencies; bitcoin & what now after liberty reserve, silk road, and Mt. Gox? *Richmond Journal of Law and Technology*, 20(4), 1–108. https://scholarship.richmond.edu/jolt/vol20/iss4/3.

Tuori, K. (2016). Crossing the limits but stuck behind the fault lines? *Transnational Legal Theory*, 7(1), 133–153. https://doi.org/10.1080/20414005.2016.1214022.

Voshmgir, S. (2017). Disrupting governance with blockchains and smart contracts. *Strategic Change*, 26(5), 499–509. https://doi.org/10.1002/jsc.2150.

Walch, A. (2019). In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains. In P. Hacker, I. Lianos, G. Dimitropoulos, & S, Eich (Eds.), *Regulating Blockchain: Techno-Social and Legal Challenges* (pp. 58–81). Oxford University Press.

Wenker, N. (2014). Online currencies, real-world chaos: The struggle to regulate the rise bitcoin. *Texas Review of Law and Politics*, 19(1), 145–197. https://heinonline.org/HOL/P?h=hein.journals/trlp19&i=157.

Winner, L. (1980). Do artifacts have politics? *Daedalus*, 109(1), 121–136. https://www.jstor.org/stable/20024652.

Wood, G. (2014). Alegality: Systems that can't care. CoinScrum and proof of work media: Tools for the future. https://www.youtube.com/watch?v=Zh9BxYTSrGU.

Woodhouse, A. (2017). "Who owns the money?" Currency, property, and popular sovereignty in Nicole Oresme's *De moneta*. *Speculum*, 92(1), 85–116. https://doi.org/10.1086/689839.

Zetzsche, D. A., Buckley, R. P., & Arner, D. W. (2018). The distributed liability of distributed ledgers: Legal risks of blockchain. *University of Illinois Law Review*, 2018(4), 1361–1406.

Zhao, X., Chen, Z., Chen, X., Wang, Y., & Tang, C. (2017). The DAO attack paradoxes in propositional logic. In 2017 4th International Conference on Systems and Informatics (ICSAI) (pp. 1743–1746). IEEE. https://doi.org/10.1109/ICSAI.2017.8248566.

Downloaded from https://academic.oup.com/policyandsociety/article/41/3/358/6529327 by guest on 07 November 2024