Blockchain and the Law: A Critical Evaluation

Quintais, J.P.; Bodó, B.; Giannopoulou, A.; Ferrari, V.

Publication date
2019

Document Version
Final published version

Published in
Stanford Journal of Blockchain Law & Policy

License
CC BY

Link to publication

Citation for published version (APA):
Quintais, J. P., Bodó, B., Giannopoulou, A., & Ferrari, V. (2019). Blockchain and the Law: A Critical Evaluation. *Stanford Journal of Blockchain Law & Policy*, *2*(1), 86-112.
https://stanford-jblp.pubpub.org/pub/blockchain-and-law-evaluation

BLOCKCHAIN AND THE LAW: A CRITICAL EVALUATION

João Pedro Quintais, Balázs Bodó, Alexandra Giannopoulou, and Valeria Ferrari*

INTRODUCTION

It is a high-risk, high-reward enterprise to write a scholarly monograph on an emerging technology when its societal use, economic worth, and even its technical design are still in flux. With little empirical material with which to work, one often has to resort to extrapolating the future developments from the myriad seed of possibilities of the present. Yet, there are moments in time when undertaking such an enterprise seems inevitable, because there is a rough consensus that the emerging technology represents more than just an incremental improvement of already existing routines, and promises—or threatens—a disruption of the status quo. Such is the case of blockchain or distributed ledger technologies. In that light, Primavera De Filippi's and Aaron Wright's *Blockchain and the Law* is a timely and valuable contribution.

The enthusiasm surrounding blockchain is understandable. The technology was born in the crypto-anarchist underground of the Internet. In less than a decade, the original Bitcoin white paper[1] was turned into a rich, functional, planetary-scale technology ecosystem in a bottom-up fashion, by a rapidly growing group of technologists, investors, and entrepreneurs, sporting grand techno-solutionist visions of how to change the world.

The blockchain ecosystem tries to build a decentralized, disintermediated, and distributed technology, which enables decentralized, disintermediated, and distributed modes of social coordination in a mostly decentralized, disintermediated, and distributed manner. This congruence

* João Pedro Quintais, Postdoctoral Researcher; Balázs Bodó, Senior Researcher; Alexandra Giannopoulou, Postdoctoral Researcher; Valeria Ferrari, PhD Candidate. All authors are affiliated with the Institute for Information Law (IViR), University of Amsterdam, and are members of the IViR's Blockchain and Society Policy Research Lab. Balázs Bodó is Head of the Lab. The authors would like to thank Daniel Gervais for comments on an earlier draft.

[1] Satoshi Nakamoto, *Bitcoin: A Peer-To-Peer Electronic Cash System*, BITCOIN (2008), https://bitcoin.org/bitcoin.pdf.

between the design of the technology, its attempted mode of development, and its stated goals is the strongest argument in favor of taking blockchain technology seriously. It explains why, despite all of the potential pitfalls, the task of assessing the social, economic and political impact of the technology should be taken up by researchers.

In contrast to less detailed and narrower previous publications on the subject,[2] *Blockchain and the Law* considers the challenges and opportunities of a blockchain-based future in the broad context of the current institutional, legal, political, economic, social, and cultural frameworks, which both shape and struggle to contain the technology. The book is keenly aware of the scope and depth of potential conflicts that would be enabled by widespread blockchain adoption. It sets out, therefore, to explore the domain of law, where many of these conflicts will likely find their resolution. The analysis orbits around the central concept of "lex cryptographica." First proposed by the authors in 2015, it refers to "rules administered through self-executing smart contracts and decentralized (autonomous) organizations,"[3] i.e. rules coded in and enforced by quasi-autonomous technological systems. Technology and law are often seen as two competing modes of ordering ever since Lessig's groundbreaking work on "code as law."[4] Software code is a powerful way to set the rules of a software-based society. But through endless legal struggles, society learned—to an extent—how to subject code and digital technology to the rule of law. Blockchain technologies, however, seem to be an altogether different beast. Because their architectural features are designed to enable the evasion of effective regulation and enforcement, they hope to elude the rule of law. The tension inherent to this process is at the heart of the book.

The book consists of five parts: on the technology; on finance and contracts; on information systems; on organizations and automation; and on regulation. We examine each part in turn, setting out the book's main arguments and critically assessing them.

I. THE TECHNOLOGY

The authors provide a clear and easily readable description of the technology—not an easy feat. Their starting point is a general introduction to blockchains, Bitcoin and decentralized platforms. The promise of the

[2] *See, e.g.*, MELANIE SWAN, BLOCKCHAIN: BLUEPRINT FOR A NEW ECONOMY (2015); DON TAPSCOTT & ALEX TAPSCOTT, BLOCKCHAIN REVOLUTION: HOW THE TECHNOLOGY BEHIND BITCOIN AND OTHER CRYPTOCURRENCIES IS CHANGING THE WORLD (2016).

[3] Aaron Wright & Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia* (Mar. 10, 2015), https://ssrn.com/abstract=2580664.

[4] LAWRENCE LESSIG, CODE, AND OTHER LAWS OF CYBERSPACE (1999). An updated version of the book was published in 2006. *See* LAWRENCE LESSIG, CODE VERSION 2.0 (2006).

technology, if successful and generally adopted, is to underpin a novel Internet architecture, often labeled “Web 3.0” (pp. 30-31). Nevertheless, not all types of blockchains are equally revolutionary, so the authors choose to focus on its truly innovative dimension: public and permissionless blockchains (p. 32).

The authors identify seven core characteristics of blockchains. First, blockchains are disintermediated and transnational networks, often relying on open-source software protocols. Second, they are resilient and tamper-resistant, due to their distributed nature, the consensus mechanisms employed, and the use of hashing. Third, blockchains are transparent—in the sense that transaction data is authenticated and visible—and the data they contain is non-repudiable (due to the use of public-private key cryptography). Fourth, they are characterized by pseudonymity, as they allow transacting parties to participate in the system without disclosing their identity. Fifth, blockchains have particular incentives and cost structures, e.g. block rewards and mining fees that incentivize and compensate parties maintaining a blockchain-based network. A sixth unique characteristic is the deployment of consensus mechanisms to coordinate social activity towards an agreement on the state of affairs within the system. Seventh, and at a deeper level, blockchains enable a specific type of “autonomy”: they facilitate the execution of software code that is entirely independent of any one party.

The combination of these characteristics leads to the observation that blockchains have a dual nature, meaning that they have the potential to be used for good and for bad. This observation underpins the remainder of the book, insofar as the authors attempt throughout their thematic analysis to illustrate this dual nature by pointing out use cases and speculating about potential beneficial and unlawful uses of the technology. For the most part, the potential of blockchains for unlawful use is tied to the fact that many of the above characteristics make it difficult to effectively bring about regulation or enforcement in a blockchain environment.

Having characterized the technology, the authors frame it within the five-layer TCP/IP model, arguing that blockchain protocols should be considered as “new application protocols that sit on top of the transport layer” (p. 48). Furthermore, such protocols and related services have the capacity to implement their own systems of rules enforced by the underlying protocol and smart contracts (p. 50). This is a central concept of the book that expressly harks back to an early vision of the Internet as a decentralized space where regulation of social relations through code can replace or circumvent “legal code.” Thus, the authors argue, should blockchain-based systems become mainstream, there will be a need to develop alternative modes of regulation (p. 52).

But mainstream adoption is far from guaranteed. From the purely technical perspective, the technology faces at least two formidable challenges: scalability and security. Blockchains are weaker and slower than existing data management technologies. Scalability in particular is difficult for what are in effect append-only databases, which require high amounts of storage, bandwidth usage and computational power. Possible solutions include moving transactions off-chain and developing faster and more efficient consensus protocols (e.g. proof of stake).[5] Still, as the authors note, such solutions have yet to materialize into viable use cases (pp. 56-57). The issue of security is developed at a later stage in the book. To these obstacles one should add that of energy consumption, largely ignored in the book. Blockchains—at least those relying on mining and proof of work—appear to be energy-inefficient and wasteful.[6] Naturally, beyond the technical obstacles, there is a plethora of non-technical barriers to the mainstream adoption of the technology, some of which are addressed in subsequent parts. Ultimately, the entirety of the book hinges upon these two assumptions: that the technical and non-technical obstacles can be overcome, and that the mainstream adoption of the technology will occur and be disruptive.

II. FINANCE AND CONTRACTS

Part II of the book discusses digital currencies and decentralized payment systems (Chapter 3), smart contracts (Chapter 4), and smart securities and derivatives (Chapter 5).

A. Digital Currencies and Payment Systems

After a brief historical note on payment systems, the book makes a case for how blockchain technology could improve payment and remittance systems. Having moved past the problem of double spending inherent to digital currencies of yore, blockchain-based cryptocurrencies are presented as appealing alternatives to countries with weak or underdeveloped payment infrastructures or remittance systems, such as Argentina, Venezuela or Zimbabwe. Potential solutions could come in the form of cryptocurrency exchange systems (e.g. Ripple) and blockchain-based remittance networks (e.g. Abra). The argument, however, is mostly theoretical. The examples provided in the book have failed to turn into compelling use cases, and to our knowledge none currently exist on the market that are of particular

[5] *Proof of Stake FAQs*, GITHUB, https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs (last visited Nov. 11, 2018).

[6] *See* Karl J. O'Dwyer and David Malone, *Bitcoin Mining and its Energy Footprint*, in ISSC 2014/CIICT (2014), 280-285.

relevance. Even for a field like remittances, where existing offerings are costly and relatively slow, the market has failed to produce a competitive blockchain-based solution.

The authors then point out the potential conflicts of digital currencies with existing laws, which arise from the distributed, transnational and pseudonymous nature of blockchains. The point is illustrated with a reference to anti-money laundering ("AML") laws, which impose monitoring obligations regarding financial transactions, often coupled with *know your client* and reporting requirements. Such obligations and requirements are not followed by most blockchain-based protocols. The tendency is for further infringement of the law with the development of pseudonymization techniques like zero-knowledge proofs and ring signatures.

A curious tension with data protection law arises here, which the book unfortunately does not explore despite multiple forays into the topic of privacy.[7] As AML regulations seek further identification of parties to a transaction—a development anathema to blockchains—data protection laws incentivize developers to push for anonymization techniques, so as to escape the increasing obligations that arise from collection and treatment of personal data, which apply even to pseudonymous data.

The book does, however, address the lack of strong privacy protections in relation to cryptocurrencies, due to their failure to guarantee anonymity, the transparency of transaction data, and the possibility of third parties mapping out the financial transactions of a given account. This, as the authors suggest by drawing a parallel to IP addresses, enables similar forms of control, surveillance and censorship. The authors' position, however, is not adequately supported by the argumentation and, in light of the current state of the technology, feels somewhat speculative.

Similarly, the remaining arguments on the possibility of mass adoption of cryptocurrencies (assuming they overcome transparency and fungibility concerns), suggesting that it would lead to a narrowing of the role of central banks in the financial system and monetary policy, are difficult to assess as they are mostly thought experiments. This is a pervasive feature of the book, which often causes the discussion to become speculative. The analytical device the authors use to deal with this shortcoming is to link their analysis to the "dual nature" of blockchains, describing the perceived best-case (blockchain for good) and worst-case (blockchain for bad) scenarios.

B. Smart Contracts

[7] *See* Michèle Finck, "Blockchains and Data Protection in the European Union," *Max Planck Institute for Innovation and Competition Research Paper* No. 18-01, 18(1) (2018), 1-30, for a good analysis of this topic under EU law.

The book then embarks on the fascinating topic of smart contracts and how blockchain-based systems have enabled this new mode of memorializing contractual arrangements (p. 72). Following a brief history of smart contracts since the development of the Electronic Data Interchange in the late 1940s—through the mandatory reference to Nick Szabo's work in the 1990s, and the possibilities of implementation of these contracts afforded by the Ethereum platform—the authors engage with the discussion of smart contracts and legal contracts.

One significant difference between *smart* and *legal* contracts relates to execution and termination. Smart contracts enforce obligations through autonomous code, i.e. strict and formal programming language (e.g. Ethereum's Solidity), wherein code is executed in a distributed manner by the nodes in the underlying network. This renders smart contracts more difficult to terminate than legal agreements, unless such termination option is properly coded into the software. In addition, the authors argue, smart contracts are more dynamic than traditional legal contracts, since performance obligations may be adjusted over time via trusted third party sources, i.e. oracles (p. 75). This latter point, however, is questionable, since many legal contracts are potentially more customizable, flexible and dynamic than smart contracts because they are not bound by limitations embedded in the self-executing code.

An intermediate category briefly explored in the book is that of "hybrid agreements," meaning the use of smart contracts to "memorialize only a limited set of promises as part of a larger, more complicated contractual relationship" (p. 77). These agreements are particularly suited for obligations that are open-ended (good faith, best efforts) or simply hard to code (like representations and warranties). Here, the authors insightfully note that the likely way forward is for smart contracts developed for binary or formulaic parts of a complex transaction to be incorporated by reference in legal contracts regulating the whole transaction (pp. 77-78).

But are agreements relying on smart contracts legally enforceable? The answer of the book is yes, at least under US law, where the key aspect is the parties' "intent to be contractually bound" (pp. 79-80). Given the fundamental importance of this question, it would have been interesting to examine it under different legal systems, e.g. EU law. Underpinned is a methodological concern regarding a book on blockchain and "the Law," since it is often not clear which "law" is being discussed save for particular instances where a brief analysis is provided under US law.

In the authors' view, the truly unique feature of smart contracts is the possibility they afford—due to their automated, disintermediated and tamper-resistant features—to contracting parties of reducing monitoring costs and the potential for opportunistic behavior (p. 80). Smart contracts provide advantages in terms of clarity, precision, and modularity. In the future, they write, we can envision a world of sophisticated smart contract libraries used not only *a la carte* in contractual arrangements but also to enable machine-to-machine transactions.

The authors identify five main limitations of smart contracts, still unresolved in the current state of the technology (pp. 83-88). First, privacy concerns, which may render them unsuitable to replace legal contracts for transactions that require confidentiality. Second, the inadequacy of smart contracts to formalize certain types of legal obligations. This includes the aforementioned open-ended provisions of ongoing relationships requiring regular updating. Third, the pseudonymous nature of parties to the contract, which raises difficulties vis-à-vis error correction and enforcement. Fourth, the widespread adoption of smart contracts may lead to standardization and a form of "automation bias," resulting in the acceptance and use of faulty contracts with limited possibilities for customization. Finally, the main problem might prove to be the potential use of smart contracts with blockchains to enable criminal or immoral activities.

C. Smart Securities and Derivatives

The authors focus on two financial products: securities and derivatives. After a brief primer on how these work, they argue that "current settlement and clearance processes suffer from operational issues," including time to settlement, counterparty risk and—for derivatives in particular—lack of transparency (pp. 91-92). In light of the 2007-2008 financial crisis and its known link to the emergence of Bitcoin,[8] there is a powerful intuition that finance is a prime field for blockchain to flourish. But can the technology truly address the above issues?

In theory, blockchains and smart contracts could streamline the settlement and clearance of securities. Blockchains could be used to tokenize a number of securities (e.g. company shares, bonds, credits) and trade them against cryptocurrencies. Smart contracts could be used to encode economic rights related to the security, thereby reducing the need for intermediaries in this field. With settlement and clearance occurring near instantaneously, there would be a reduction in counterparty risk and disputes (pp. 93-94). Likewise, blockchains could facilitate the creation, execution, and trading of derivatives; however, since these instruments rely on future events, they would necessitate third parties (such as oracles) to adjust contractual performance (p. 95). Still, despite many ongoing experiments, in this field too there is a lack of use cases to make good on the promise

[8] *See* Satoshi Nakamoto, *Bitcoin open source implementation of P2Pcurrency* (2009), http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source (last visited Nov. 11, 2018).

sketched out by the authors. In multiple jurisdictions (New York, Switzerland, Gibraltar, Malta), financial regulators issued guidance or straightforward regulation that applies to cryptocurrency-based intermediaries (such as exchanges) or practices (e.g. Initial Coin Offerings or "ICOs").[9] Yet, despite an arguably higher level of legal certainty, and the presence of innovation-friendly regulatory environments, the current cryptocurrency financial infrastructure lacks the depth and sophistication of its fiat currency-based counterparts.

The main limitations of smart securities and derivatives is that blockchains are not clearinghouses and do not provide insurance to market participants.[10] Therefore, if generally adopted, they may increase the systemic risk of the financial sector. If that is the case, one wonders whether—even at the largely theoretical stage we encounter ourselves in—it makes sense to pursue and promote the adoption of smart securities and derivatives.

This doubt is somewhat reinforced by the authors' argument on the potential of blockchains to support unlawful decentralized capital markets (p. 98). Here, the authors discuss the legality of fundraising mechanisms in this field, like "token sales" or ICOs, through which large amounts of money have been raised by blockchain-based ventures since 2014. They note the regulatory trend (in the US, Singapore, China and South Korea) of considering at least certain token sales as subject to securities law frameworks (pp. 101-102). Despite this, such token sales are difficult to shut down due to the architecture of blockchains, which the authors analogize, "do to securities law what the Internet did to copyright law" (p. 103). They conclude that similarly to payment systems and legal agreements, blockchains can bring about benefits to financial markets (e.g. reducing intermediation and automating certain routine aspects), as well as drawbacks (e.g. enabling peer-to-peer circumvention of rules and regulations) (p. 104).

III. INFORMATION SYSTEMS

Part 3 of the book is developed around one distinguishing characteristic of the blockchain: tamper resistance of the distributed database. The authors envisage types of social change that could stem from potential applications of this characteristic of the technology; all while presenting the implications that these applications can have for our social norms and regulatory approaches. In their view, reliance on *lex cryptographica* will have a

[9] Wulf Kaal, *Initial Coin Offerings: The Top 25 Jurisdictions and their Comparative Regulatory Responses (as of May 2018).* 1 STAN. J. BLOCKCHAIN L. & POL'Y 41 (2018).
[10] Other limitations are related to how transparency of blockchains may hinder the protection of confidential information of financial services firms and lead to "weaker corporate governance practices" (pp. 97-98).

transformative effect on society by eliminating the need to organize norms and enforcement around central actors. They predict that the effects of this transformation will be positive, despite the risks related with the absence of control and redress mechanisms. The analysis delves first into tamper-resistant, certified and authenticated data (Chapter 6), describing a society where blockchains could be applied in a complementary manner to the public sector and the state. It then examines resilient and tamper-resistant information systems based on blockchain technology (Chapter 7), viewing them as a more independent mechanism of information dissemination that has very little connection to specific jurisdictions or regulatory frameworks.

A. Tamper-Resistant Data

Can the current system and existing institutions benefit from using tamper-resistant and resilient repositories for public records and other types of authenticated data and certified information? In discussing tamper resistance, the authors state that "blockchain is a transparent and sequentially organized database that is resilient and resistant to change … It can thus serve as a certified source of permissions—an access control mechanism—that can be used to determine whether a party is entitled to view, share, or modify data" (pp. 109, 112). The overarching example used to illustrate the consequences of using a resilient and tamper-resistant database is that of public records. After highlighting the current system's failings, the authors describe the advantages and shortcomings of using blockchain-based systems for safeguarding, processing, and sharing public records.

More specifically, they expand on two use cases and their effects: land registries and public records of sensitive information. First, there are current practical examples where the blockchain is being explored as a solution for land registries (e.g. ongoing projects in Illinois (US), Sweden, the Republic of Georgia, and the Republic of Ghana). There are multiple advantages in creating a decentralized tamper-resistant database of public records according to the authors. Namely, such a database could facilitate and ensure the quality of real estate transactions, prevent corruption and fraud, and promote citizen trust and transparency. At a higher level, the authors envisage potentially "unified global title recordation systems" that could facilitate international transactions of land "in minutes" to the point of making them as simple as a Bitcoin transaction. However, it is difficult to relate to the given example because of the nuances of on-chain and off-chain synchronicity and other complexities in creating such a system, only briefly mentioned by the authors.

The second use case is for maintaining public health records or sensitive data in general. Such an application will have, according to the authors, significant security benefits for the government, as it will permit the continuous verification of the integrity and authenticity of the sensitive information at hand by facilitating the identification of malicious attacks, corruption attempts, and inconsistencies. The authors claim that managing sensitive health data through the blockchain can permit greater data control for the data subjects. From the government's perspective, blockchain can create a process of verifiable certification of data while maintaining the security required due to the nature of the data. It can also enable the creation of granular access permissions to data. However, and as the book rightly points out, blockchains are not immune from corruption. Tamper resistance is only necessary when the quality of the data input to the database can be trusted. After all, "[r]egistries and recording systems are only as good as the information they manage" (p. 114). Malicious attacks and mishandling of key management can permit the storage of inaccurate information or the inability to finalize the recordation of a transaction. Without institutional support through the intervention of intermediaries holding a verification role, these processes are unlikely to succeed.

The authors then proceed to illustrate shortcomings of such processes from a privacy perspective. The tamper resistance and the fact that data are stored on the blockchain indefinitely pose a significant privacy risk. The inferences that parties can make by processing the data publicly stored in a transparent blockchain further exacerbate the privacy dangers for individuals. Consequently, the issue of the type and nature of data that should be stored on the blockchain is central in assessing privacy and security threats on blockchains.

The chapter remains true to the declared goal of illustrating applications and effects of tamper-resistant blockchains in current and future use cases of blockchain-based projects. The authors provide an overview of different conflicts that arise from implementing blockchain-based systems on public records. These include, for instance, trust in the data inserted in the blockchain, privacy, and security. Still, the authors choose to not go in-depth on any of these issues. The projects and applications mentioned (such as the public records systems implementation proposals in some countries or the authors' example of assisting claims of the Syrian people over their land) hold a quasi-prominent role in the chapter, representing an admittedly techno-solutionist approach to issues concerned with the relationship of existing institutions and blockchains. From the reader's perspective, instead of solidifying an underlying techno-legal argument, they distract from the overall structure and from the original purported goal of providing a legal analysis of the underlying confrontations. The reader thus becomes perplexed while trying to follow the legal issues that the chapter is trying to highlight.

The authors conclude that external recognition of a blockchain system through complementary use of the technology by the already existing institutions is risky but beneficial; however, at the same time, the argumentation appears contradictory and difficult to reconcile with the book's overarching theme of applying *lex cryptographia*, which purports the elimination of the role of existing institutions. Furthermore, important issues related to data privacy are only briefly mentioned. When they are, no distinction is made concerning the significant differences in data protection rules across legal systems. In particular, the lack of reference to the stricter European regulatory framework under the General Data Protection Regulation is regrettable.

B. Tamper-Resistant Information Systems

The book then moves to a discussion on information systems. Here, the blockchain is described as "underlying new systems that aim to break down the 'barbed wire' of copyright law while simultaneously supporting platforms that could help spread indecent, obscene, or inflammatory information" (p. 117). The authors take examples from information law related to the current state of Internet actors in order to showcase the advantages and imperfections of applying blockchain technology for the free flow of information. Departing from the premise that the current system of centralized intermediaries permits increased control of the type of information users are able to access, the authors present use cases of blockchain applications that foster the free flow of information.

For instance, the authors explain how smart contracts can be combined with peer-to-peer or overlay networks to enable file-sharing by storing on the blockchain the actual information or simply a reference to a file available elsewhere. The latter option simultaneously creates a tamper-resistant record of the data stored without forcing the exponential growth of the blockchain record. By presenting use case examples of content dissemination through tokenization (such as Alexandria and Lbry), the authors envisage a wholly blockchain-based system "governed by *lex cryptographia*" that could "provide access to large repositories of music, films, images, and books hosted on millions of computers across the globe in an easily accessible and searchable format" (p. 120). While showcasing the multiple benefits of such a system to facilitate the free flow of information and free speech, the analysis briefly points out the risks inherent in over-reliance on blockchain technology for the management of information.

Despite the widespread use of TOR, and other privacy-enhancing technologies which have the same effect, the authors suggest that the most significant risk of blockchain-based applications in this domain is the creation of censor-resistant communication. That is to say, communication that is not subject to centralized intermediary control regulating copyright or free speech, even where such regulation or control would be justified or desirable. The reliance on *lex cryptographica* would suffice to circumvent external control from regulatory parties or intermediaries, making enforcement difficult. From the authors' perspective, even in those instances where liability for the unlawful conduct could be found (or attributed), private or public enforcement through injunctions would be challenging. In general, dissemination of information and content through blockchain-based decentralized communication systems makes impossible enforcement against illegal or unlawful content, whether copyright infringement, harmful speech (including hate speech), or even information related to national security. Ultimately, there is a need for such blockchain-based systems to strike a balance between free flow of information and broad social costs of public order and morality.

The chapter's overall structure is not ideal. Its oscillation on the subject of free flow of information between content dissemination, communication, and free speech weakens the argument. With the role of real-life use cases less visible in the foreground, the argument brought forward appears speculative due to the lack of sound legal analysis. More specifically, taking examples from diverse and admittedly challenging areas of law such as copyright enforcement against decentralized networks and free speech regulation, the authors hastily conclude that due to a mismatch between regulation and blockchain technology, the natural evolution will be that of reliance on the rule of code for regulating (or not) the dissemination of information. The overview of a significant amount of legal issues, varying from regulating free speech in a transnational distributed environment and enforcing copyright in a system that has no central actors, to protecting personal data and privacy in a transparent decentralized database, does little to reveal the underlying complexities and age-old questions related to the interactions of law and technology.

IV. ORGANIZATIONS AND AUTOMATION

Part 4 of the book seeks to explain the potential of blockchain technology to "facilitate social interactions and commercial activity in ways that were not possible before" (p. 131). To do so, the text browses and criticizes blockchain-based governance solutions in a number of scenarios, namely with respect to corporations and existing organizations, decentralized organizations (Chapter 8), decentralized *autonomous* organizations (Chapter 9) and, lastly, the Internet of Things (Chapter 10).

A. The Future of Organizations

The authors first tackle the potential of blockchain for organizational and governance solutions. The analysis starts with an archeology of "organizations" as forms of coordination between individuals who pursue common economic goals—their main function being that of lowering transactions costs. Organizations aim to decrease the number of operations required to perform specific tasks, as well as to reduce the chances of opportunistic behavior in upholding mutual contractual commitments. Nevertheless, organizations themselves generate new forms of complexity, to the point that internal operational costs may outweigh those of external market transactions for the same tasks. Here is where the authors think blockchains can add value. In particular, the deployment of blockchain-based smart contracts to automate the implementation of organizations' internal rules and procedures presents advantages. Aggregating rules within a smart contact would not only increase the efficiency and transparency of internal operations, but also the involvement of shareholders in decision-making processes and the responsiveness of the legal entity as a whole. Smart contracts could be used to automatically distribute tokenized economic and voting rights, reducing the opportunity for fraud and miscalculations.

This part of the analysis describes the potential of blockchains to improve organizational models for corporations. However, it showcases solutions without describing the technical and legal processes that such solutions would entail. In particular, the tokenization of voting rights and companies' shares—which seems to be most innovative feature blockchains can provide in this context—deserve a deeper analysis. Given the growing interest in blockchain technology from established and emerging companies, the book also could have better explained the economic incentives for the deployment of the technology and the applicable legal frameworks.

In a subsequent section of the analysis, the authors present the concept of decentralized organizations. Whereas, broadly speaking, the rigidity of blockchains provides "an additional layer of accountability" in organizational transactions (p. 135), they could underpin not only "incremental improvements to existing corporations," but also new types of organizations—what the authors call "decentralized organizations." Relying on blockchain technology and smart contracts "as their primary or exclusive source of governance" (p. 136), these are described as an extension of open-source organizations: networks of individuals that, coordinated by the blockchain protocol, work toward a shared social or economic goal. Within these entities, governance processes and members' rights—distributed as cryptographic tokens—are managed via smart contracts, allowing all shareholders to take part in decision-making processes. The *lex cryptographica* that governs such entities can be designed to coordinate members' activity "in a transparent and inclusive manner" and "for the benefit of its participants rather than a central intermediary" (p. 139).

While blockchain-mediated decentralized organizational models may be less efficient than hierarchical forms of coordination, their real value seems to lie in the possibility to experiment with new forms of governance that were previously impossible to implement at a large scale. However, such blockchain-based governance models are not without issues. First, the authors foresee security challenges, as smart contract code "is not immune to human error and could incorporate vulnerabilities that could be exploited by third parties" (p. 141). Second, decentralized organizations and financial assets circulating within them will raise new, significant legal challenges, such as the lack of limited liability for shareholders and the applicability of national security regulations; these clash with the global, pseudonymous and decentralized nature of decentralized virtual entities. Finally, as the authors again note, regulation of such organizations is challenging, as it will be difficult to subject them to traditional enforcement measures and sanctions.

A merit of this part of the analysis is that it succeeds in outlining the concept of decentralized governance to neophytes. Still, the authors struggle in relating their explanation to real-world applications. The examples provided—TheDAO and MakerDAO—are entities whose legal status and socio-economic objective remain unclear. The argument for decentralized governance would have been stronger with a better identification of the legal entities and economic relationships to be reshaped by blockchain technology. Further details on the factual governance solutions deployed by decentralized organizations would have been welcomed, together with an assessment of their possible legal treatment. For instance, it would have been appropriate to engage here with the scholarship on the application of corporate governance solutions to address the lack of formal governance in open and permissionless blockchains.[11] The authors further claim that deterministic blockchain-based governance systems would allow for transparent and inclusive decision-making systems (p. 139). However, this claim is not examined against the possible limitations arising from plutocracy and futarchy models dominant in ongoing experiments on decentralized governance. As the authors recognize, these systems are typically (and to a certain extent necessarily) based on individual incentives that associate voting rights to stakes (p. 137). As such, they allow for the concentration of decision-making power, creating a risk of conflict with the stated intention of improving the "democratic proprieties" of organizations

[11] *See* Philipp Hacker, *Corporate Governance for Complex Cryptocurrencies? A Framework for Stability and Decision Making in Blockchain-Based Organizations*, *in* REGULATING BLOCKCHAIN: TECHNO-SOCIAL AND LEGAL CHALLENGES (Philipp Hacker et al. eds., forthcoming 2019), *available at* https://ssrn.com/abstract=2998830. To be clear, the authors do recognize the lack of governance in public permissionless blockchains (e.g. at p. 27).

(p. 140). Finally, from a legal perspective, the overreliance on decentralization as a means to escape the reach of law enforcement leads to a superficial analysis of other legal issues (beyond limited liability and the applicability of securities law), which deserve a more thorough examination.

B. Decentralized Autonomous Organizations

Moving forward the discussion on blockchain-based forms of organization, the book then examines the concept of *decentralized autonomous organizations* ("DAOs"), which are not governed by humans or consensus groups but by autonomous, deterministic code and artificial intelligence ("AI") systems. DAOs can vary in scope and level of sophistication, their common denominator being that activities and processes are executed by algorithms running autonomously on the blockchain. The predeterministic rules governing the DAO can be "designed to serve the interests of the company's shareholders," increasing overall efficiency and reducing opportunities for opportunistic behavior (p. 152). However, they do not come without risks. While DAOs' greater efficiency can result in economic benefits for consumers (or producers or owners), their competitive advantage over traditional organizations could result in monopolies and concentration of power: "If DAOs surpass traditional human-run organizations, we could be left, as a society, in a situation where people are collectively worse off" (p. 153). DAOs also raise complex legal challenges, such as the jurisdictional issue linked to their decentralized, world-wide dimension. Furthermore DAOs lack of legal personhood create challenges to the attribution of duties and rights requiring such status. Last but not least, even if legal liabilities could be imposed on DAOs, problems of enforcement remain, as the autonomous code can continue to execute illegal activities without third parties being able to prevent it.

While we agree that DAOs provide a fascinating object of analysis, the analysis would have benefited from a more critical approach towards the feasibility and desirability of DAOs. The emergence of DAOs in the near future is presented as preordained, leaving the reader with the question of who would have a stake in setting up organizations that are "increasingly untethered from human control" (p. 147). An examination of use cases would have been welcomed, so as to understand which incentives determine the degree of elements of human control in decentralized organizational structures. Moreover, there is little to no reference to the significant amount of scholarship criticizing automated governance and algorithmic decision-making, such as that focusing on instances of discrimination.[12]

[12] *See, e.g.*, Jack M. Balkin, *The Three Laws of Robotics in the Age of Big Data*, 78 OHIO ST. L.J. 1217, 1217, 1219 (2017); Amanda Levendowski, *How Copyright Law Can Fix Artificial*

C. Blockchain of Things

This part of the book concludes with an analysis of the implications of deploying blockchain as a "common application layer" to execute smart contacts and store information to feed the operations of Internet of Things ("IoT") devices (p. 158). It is argued that blockchains can provide better interoperability and security of IoT systems as compared to current centralized offerings. Building on this argument, the authors discuss how blockchains could enable devices to autonomously transact value among each other on a peer-to-peer basis. Devices could "turn into services themselves," with governance rules, terms of use and even commercial strategies embedded in their technical design (p. 159). The futuristic scenario envisioned in the book is that of a new generation of applications and services (e.g. blockchain-enabled rental marketplaces) provided through multiple connected devices interacting via blockchain-based smart contracts without human intermediation.

Imagining services that entail commercial interactions between devices opens the issue of the legal treatment of such interactions and the agents involved. In this regard, the authors note, as long as the actions of an "electronic agent" are attributable to an identifiable party, no blockchain-specific liability issue arises. However, with a combination of blockchain and AI, "[i]n a matter of decades, machines could operate in a manner that is independent of any third-party operator" (p. 165). In this scenario of emancipated devices, existing liability rules may not suffice, and "new legal and ethical questions will emerge" (p. 168). One possible approach discussed by the authors to liability questions relating to these autonomous machines is the recognition of their legal personhood, so "as to give them the ability to acquire specific rights and obligations that are enforceable under the law" (p. 168). But if autonomous devices are based on a blockchain and powered by smart contracts, the enforcement challenges noted above remain, since no third party—including courts—would be able, e.g., to control or seize the devices' assets. The authors conclude with a warning: any sort of autonomous, AI-driven machine (including automated weapons systems), could be created, and once implemented, keep functioning with no human ability to stop its operations—unless the underlying smart contract provided such functionality (p. 169).

The forward-looking nature of the analysis of a blockchain of things is necessarily tricky, as it is a hotbed for speculation. The reliance on

Intelligence's Implicit Bias Problem, 93 WASH. L. REV. 579 (2018); Mireille Hildebrandt, *Learning as a machine: Crossovers between humans and machines*, 4 J. LEARNING ANALYTICS 6 (2017).

autonomous machines that operate independently from third-party influence or control seems to be described as a manna that solves problems of efficiency, reliability and liability, and can even ensure "perfect enforcement" in connection to a particular device (p. 163). However, the implications of such an ex-ante enforcement approach to individuals' rights and freedoms are not discussed beyond the risk of depriving "consumers of the right to use property as they see fit" (p. 169). The massive reliance on algorithmic-based decision making that is proposed—for potential use not only by private parties but also governments—entails risks in terms of privacy, autonomy, discrimination and consumer protection. Such risks are well-documented, for example in scholarship on AI and algorithmic regulation, but largely ignored here.[13] While acknowledging the powers of manufacturers to determine the extension of property rights and connected privileges of users over devices, the authors do not discuss any possible legal treatment of such manufacturers. Instead of examining problematic real-life possible application, the authors propose an example—that of the *plantoid* (information about the project is available at http://okhaos.com/plantoids)—which more than an IoT product or service resembles an artistic experiment (pp. 166-167). Finally, as in the discussion on DAOs, the legal analysis focuses on the legal personhood of autonomous devices. From a legal perspective, however, the analysis misses the necessary preliminary discussion on the ecosystem of stakeholders operating behind the technology, as well as their potential liability.

V. REGULATION AND CODE

Part 5 of the book discusses some aspects of the regulation of decentralized blockchain-based systems, under the headings "modes of regulation" (Chapter 11) and "code as law" (Chapter 12).

A. Modes of Regulation

Modes of regulation are described as the ways in which the State can regulate the design and operation of decentralized blockchain networks, and enforce its own rules enshrined in laws. The chapter uses Lessig's "pathetic dot theory," introduced almost two decades ago,[14] to discuss the opportunities of the State to regulate blockchain technology through laws,

[13] *See, e.g.*, MIREILLE HILDEBRANDT & KATJA DE VRIES, PRIVACY, DUE PROCESS AND THE COMPUTATIONAL TURN (2013); Karen Yeung, *Blockchain, Transactional Security and the Promise of Automated Law Enforcement: The Withering of Freedom Under Law?*, *in* 3TH1CS: A REINVENTION OF ETHICS IN THE DIGITAL AGE? (Philipp Otto & Eike Gräf eds., 2017); Karen Yeung, *Algorithmic regulation: A critical interrogation*, 12 REGULATION & GOVERNANCE 505 (2018).

[14] *See* LESSIG, *supra* note 4.

social norms, market intervention and code. When it comes to laws, the authors focus on the points at which the State can interfere with the operation of a decentralized technology network.

The book discusses in brief a panoply of pros and cons (pp. 175-184): of regulation of end users; of the transportation layer; of general internet intermediaries, like ISPs and blockchain-specific ones, such as cryptocurrency exchanges; of miners and other constituents of the blockchain network; of hardware manufacturers; and of the code itself. The analysis then turns to the advantages and difficulties of regulating blockchain technologies through other means. Market forces are understood as the State buying and selling cryptocurrencies through direct market intervention, to raise or lower the cost of services which these tokens make accessible. Regulation through social norms is understood as the governance *of* the technology, and the procedures, institutions, and logics of decision-making within the developer community (p. 187). The regulation of/through architecture is discussed as an opportunity to require certain functions (such as backdoors) to be inserted into the code, the implementation of code certification procedures, or government-producing code. The analysis concludes with a short discussion of some regulatory tradeoffs (p. 189), most notably the presupposed tradeoff between regulation and innovation, claiming that an overly zealous regulatory approach may stifle innovation in end-to-end networks, unregulated software domains, and markets.

A chapter on the modes of regulation would seem like the focal point in a book on blockchain and the law. Yet, the authors made some curious choices, which in our view limit the power of their analysis. First, the detailed and convincing account of how blockchains can ultimately be regulated seems to contradict the argument on which the book so far has been based, namely that blockchain technology is difficult, if not impossible to regulate. In a way, this argument undermines many of the use cases and purported benefits of the technology advanced throughout the book.

Second, the regulation (or perhaps the governance) of techno-social assemblages with a decentralized technology at their heart is a problem as old as the printing press, if not older. A large number of concrete regulatory frameworks and an even larger number of scholarly analyses are available to discuss this problem both on a general level, and in fine detail.[15] The regulability of peer-to-peer networks was raised and elaborated in the

[15] *See, e.g.*, JACK L. GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD (2006); *Towards a Collaborative, Decentralized Internet Governance Ecosystem: Report by the Panel on Global Internet Cooperation and Governance Mechanisms,* ICANN (May 21, 2014), https://www.icann.org/en/system/files/files/collaborative-decentralized-ig-ecosystem-21may14-en.pdf.

context of copyright enforcement.[16] Regulatory tradeoffs between enabling a certain level of criminal activity in exchange for the safety and security of online communications were extensively discussed in the context of the TOR privacy-enhancing technology and other PETs.[17] The growing prominence of the "sharing economy"—the rise of online platform monopolies that pool distributed resources—prompted lively debates about how such planetary-scale technology infrastructures could be made to comply with a myriad of local, often conflicting regulations, including speech regulations, labor laws and anti-discrimination rules.[18] The debates concerned their role in the monitoring of the behavior of their users[19]; their obligations to enforce laws vis-a-vis third parties; and their role in cyber warfare and the general provision of cyber-security (see the debate on the platforms' role in preventing interference after the 2016 US presidential elections). Yet, little of this literature is referenced in Chapter 11. To be sure, addressing all of these issues in detail would have gone beyond the book's scope. But it would have made sense—especially in light of the book's title—to at least draw some of the possible parallels with past debates on regulating and governing transnational, decentralized technology/communications networks, and to discuss a select few in depth. As it stands, the reader is presented with the notion that the problem of regulating blockchain technologies is something altogether new and unique, while it is arguably neither.

Third, the chapter frames regulation as a possible threat to innovation and development. Again, this is a very US-centric approach, and even then, its validity is questionable.[20] The US has traditionally had a much more antagonistic approach to government regulation than, for example, Europe. A wide spectrum of arguments and ideologies are being constantly mobilized to refute possible government interference with corporate or individual autonomy. In that context, the supposed conflict between innovation and regulation uncritically echoes the libertarian ideology so

[16] *See* R. K. GIBLIN, CODE WARS: 10 YEARS OF P2P SOFTWARE LITIGATION (2011); WILLIAM PATRY, HOW TO FIX COPYRIGHT (2012).

[17] *See* Damon McCoy et al., *Shining Light in Dark Places: Understanding the Tor Network BT, in* PRIVACY ENHANCING TECHNOLOGIES 63 (N. Borisov & I. Goldberg eds., 2008),; Michael Chertoff, *A public policy perspective of the Dark Web*, 2 J. CYBER POL'Y 26 (2017); Monique Mann & Ian Warren, *The digital and legal divide: Silk Road, transnational online policing and Southern criminology, in* THE PALGRAVE HANDBOOK OF CRIMINOLOGY AND THE GLOBAL SOUTH 245 (Kerry Carrington et al. eds., 2018).

[18] *See* Pieter Nooren et al., *Should We Regulate Digital Platforms? A New Framework for Evaluating Policy Options*. 10 POL'Y & INTERNET 264 (2018); Victoria Nash et. al, *Public Policy in the Platform Society*, 9 POL'Y & INTERNET 368 (2017) (for an overview).

[19] *See* S. Zuboff, *Big other: surveillance capitalism and the prospects of an information civilization*, 30 J. INFO. TECHN 75 (2015) (on surveillance capitalism).

[20] Knut Blind et al., *The impact of standards and regulation on innovation in uncertain markets*, 46 RESEARCH POL'Y 249 (2017).

prevalent in the blockchain developer and user community.[21] To the extent that the impact of the cyber-libertarian, crypto-anarchist roots of the community on the architecture of the technology requires critical reflection, so could the regulation vs. innovation argument use a more critically informed analysis. Regulation does not *necessarily* need to stifle innovation. On the contrary, multiple studies argue that innovation depends on a number of conditions regulation provides: legal certainty, strong property rights, contract enforcement, and the ability to resolve collective action problems.[22] These issues also heavily affect the nascent blockchain domain, so one must wonder if the blanket rejection of regulation to favor innovation is a useful approach without taking into account what types of regulation might actually aid innovation in different countries and jurisdictions.

Fourth, as we also discuss below, a more nuanced understanding of the concept of regulation could have revealed that the conflict is not about to what extent governments can or should regulate blockchain technologies. Instead one could argue the real struggle is between, on the one hand, private modes of regulation (self-regulation of platforms, businesses, and technology networks) and the private ordering they enable, and on the other hand, the rules devised and enforced through democratically accountable processes and institutions. The question is therefore not whether one will replace the other, but rather what kinds of logics may enable private modes of ordering to dominate in certain domains, at the expense of democratically negotiated and accountably enforced rules.

This leads us to our last point concerning this chapter: i.e. the language which is used to discuss the problems of regulation. The chapter refers to regulation as the ability of the State to impose its will on a technology. The discussion mostly focuses on the technological dimensions of regulability, i.e. those technical characteristics which prevent or enable the enforcement of laws by the State. The same question looks quite different when discussed from a legal perspective.[23] From that perspective, the understanding of technology is but a first step towards addressing substantial legal questions. These include questions on applicable law, competent jurisdiction, identification and legal standing of parties to an agreement, contractual and statutory obligations, or the exposure to liability by different parties in the blockchain ecosystem. Any arrangement or situation will need to clarify these questions (and more) if it wants to be intelligible in legal terms. A good illustration of this point is the extensive discussion on the conflict between the architecture of blockchain technology

[21] DAVID GOLUMBIA, THE POLITICS OF BITCOIN: SOFTWARE AS RIGHT-WING EXTREMISM (2016).

[22] MEHMET UGUR, GOVERNANCE, REGULATION AND INNOVATION. THEORY AND EVIDENCE FROM FIRMS AND NATIONS (2013).

[23] B. AUDIA ET AL., THE LEGAL ASPECTS OF BLOCKCHAIN (2018).

and the legal rules in the EU's General Data Protection Regulation.[24] Other examples include the regulatory challenges around open-source software, or the regulation of Internet-enabled cross-border criminal activities. Yet, such analysis is largely missing from the book.

B. Code as Law

After examining regulation *of* technology, the book's final chapter is concerned with regulation *by* technology. It discusses some of the issues around embedding laws in computer code and other technological systems that regulate human activities. According to the authors, the promise of blockchain technology in this domain is twofold. First, on the infrastructural or protocol level, the decentralized, tamper-proof nature of blockchains promises that technology can act as a neutral, incorruptible arbiter and enforcer of rules embedded in it. Second, the smart contract layer on top of the basic blockchain infrastructure gives private parties the opportunity to implement private ordering regimes, also neutral and incorruptible (pp. 196-199).

The authors list some of the supposed advantages of such code-based legal systems: efficiency; higher levels of predictability and consistency; less uncertainty and ambiguity in the interpretation of rules; and ultimately the customizability of rules. Blockchain code is also said to be able to monitor legal compliance, as well as to automate and uniformize enforcement in a non-discriminatory manner. There are of course limitations to the "code as law" approach. For instance, it may prove hard to transpose deliberately ambiguous and open-ended legal rules into unambiguous and deterministic technical code. The powers of interpretation and discretion are deeply ingrained features of our legal systems, but hard to implement in rigid code-based systems. Furthermore, automatic enforcement removes the State's or private parties' discretionary powers regarding how to apply laws in specific contexts, or regarding breach of contract when that is a more efficient course of action. The vulnerability of code to gaming, exploitation, or hacking is also a recurring issue. Algorithmic personalization of rules and laws raises issues with other fundamental values in the legal and justice system, such as formal equality before the law.

The authors identify efficiency as the main advantage of code-based regulatory systems (p. 198), but do not elaborate what they mean by that concept. Therefore, one wonders, what exactly is the source of the supposed efficiency gains for blockchain-based systems—or more generally,

[24] *See* Michèle Finck, *supra* note 7; COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (CNIL), *Solutions for a responsible use of the blockchain in the context of personal data* (Nov. 6, 2018), https://www.cnil.fr/sites/default/files/atoms/files/blockchain.pdf.

algorithmic decision-making—and rule enforcement systems? If the source of efficiency gains is the lack of human oversight or discretion, or users' limited ability to question, contest, dispute and redress algorithmic decisions, then the question we should ask is not if such a system is technically possible or efficient, but whether it is desirable.

There is growing empirical and theoretical scholarship on the operation and impact of automated, algorithmic systems in the public sector, in the domains of policing, welfare, health care, and in the private sector, as used by insurance companies, credit rating agencies, search engines, etc.[25] From these studies it is clear that such systems are far from what they were hoped to be: a neutral, unbiased, fair judge, and enforcer of rules. It is increasingly evident that it is very difficult—if not impossible—to address the explicit and implicit biases encoded in algorithmic systems. As long as such biases exist, it is reasonable to demand *more* (not less) human oversight when public and private actors start to delegate some of their authority to algorithmic systems. Despite the wealth and depth of the debates on AI, data governance, surveillance capitalism, predictive policing, algorithmic discrimination, and related fields, there was little effort to link these to the issue of regulation through blockchain technologies.

We must also ask whether regulation through blockchain technology is actually the rigid, immutable, auto-executing enforcement machine portrayed in the book. We suspect that in addition to this strict enforcement regime, blockchains also mobilize another, completely different regulatory regime, based on economic incentives. After all, blockchains incorporate a complex system of crypto-economic incentives in the technology's design. Crypto-economics tries to encode game-theoretical insights into the software infrastructure to encourage certain behaviors, while discouraging others. Many inherent features of blockchain technology, like immutability, are achieved not through making them technically impossible, but through the disincentivization of cheating, namely by making undesirable behavior prohibitively expensive. Moreover, as the recentralization on various layers of decentralized blockchain technology is taking place, subtle crypto-economic disincentives are being built into some of the protocols to prevent concentration of activities, and the collusion of actors.[26] Despite its apparent centrality to the operation of blockchains, crypto-economics is only mentioned in a single footnote, which is a surprising omission.

On a related note, the analysis in this part of the book interprets regulation as the ability of the State to impose its will on a technology

[25] Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact,* 104 CAL. L. REV., 671 (2016). For a more recent overview, *see* VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR (2018).

[26] *See, e.g.*, Vlad Zamfir, *The History of Casper — Chapter 4,* MEDIUM (Dec. 12, 2016), https://medium.com/@Vlad_Zamfir/the-history-of-casper-chapter-4-3855638b5f0e.

through various modes of coercion. Regulation is framed as a battle between code and law, between the State and a technology. Yet, we know that such artificial separations rarely offer a useful frame to understand how certain social, economic, political, and human domains are ordered, how power is both organized and organizes the relationships among different constituents. As Foucault argued, the State—with its juridical powers to repress—is hardly the only (and often not even the most) important player in the complex network of different institutions, practices, and technologies, which through their interactions, struggles, and competition shape the order of things.[27] This statement seems especially applicable in a domain where digital technologies are prominent: powerful, cross-border, and networked technologies aggregate the activities of innumerable different constituents, including private and public actors. In turn, these technologies are operated by a handful of multinational corporations, like Google or Facebook (at least in Western societies), which are often strong enough to push back governmental efforts to regulate them, but sometimes yield to random insurgencies of their employees or users on some finer details of their codes of conduct and terms of service. Computer code can hardly be isolated from this complex network as an autonomous agent. Neither does it make much sense to equate power with the State alone. Consequently, the juxtaposition of software code (and the coders) next to the law and the State which produces and enforces it is of limited use in addressing the challenges posed by blockchain technologies and other decentralized techno-social assemblages.

CONCLUSION

The reader may be familiar with the infamous, fan-produced trailer for Stanley Kubrick's *The Shining*, which was edited to present the horror movie as a fuzzy, warm romance-comedy. The trailer is an eternal reminder that from the very same elements, completely different, often contradicting stories can be told. *Blockchain and the Law* is structured to start with the speculative, enthusiastic scenarios of what the technology could do, and to focus on the shortcomings, difficulties and limitations in the second half. The result is a book with a very optimistic—even enthusiastic—view of blockchain technology, and a rather skeptical and critical approach to (State) regulation. This approach roughly corresponds to the predominant US- and technology-centric narrative, which tends to view technology as a solution to problems governments come to represent: oppression, inefficiency, coercion, etc.

[27] Michel Foucault, *Truth and Power*, *in* THE ESSENTIAL WORKS OF FOUCAULT, 1954-1984, VOL. 3 (James D. Faubion ed., 2001).

The authors of this review come from a different tradition. We are skeptical about unbounded techno-solutionism,[28] and we prefer a critical approach to technology, the agendas that drive its development, and the ways in which one imagines that it can transform society. As Europeans, we are not averse to regulation; as legal scholars, we are very aware of the importance of nuance and detail. From this perspective, the elements from which De Filippi and Wright build their optimistic blockchain narrative could be used to produce a rather different, much more skeptical, and certainly more complex and critical, picture. It is too early to say which approach will ultimately prove correct. Therefore, rather than arguing the merits of blockchain technology, we conclude this review with a note on some of the methodological issues relevant for any debate centered on the regulation of technology, and the "the code vs. the law" dilemma. The question of how to regulate a decentralized technology is not limited to blockchains. It may thus be useful to identify some of the pitfalls in this debate, using blockchain technology to illustrate broader concerns.

One of the recurring narratives of technology regulation, which is also characteristic of this book, is to pit regulation by code against regulation by law. This creates antagonistic, often binary, and mutually exclusive relationships between two narrowly defined alternatives: the state vs. blockchain, law vs. code; lawyers vs. coders; and centralized institutions vs. decentralized, self-organizing 'autonomies.' While it is appealing to present the problem of technology regulation as a struggle between two autonomous, independent, and antagonistic powers, we believe that in practice this is not usually how the two relate to each other. Different modes of economic, social, political, cultural, and architectural modes of organization can coexist, cooperate, and organize themselves into mutually dependent networks.[29]

The State and the technology (developers) are two members of a much larger group of constituents of our networked, digital, information societies, where different stakeholders follow different agendas, respond to different incentives, and interact in dynamic—often unforeseeable—ways. The fact that such complex systems are hardly deterministic doesn't limit scholarly and other speculation about what *could* happen. Instead, it is within our reach to identify at least some of the conditions and logics that shape the development of such complex techno-social systems, and use them as a starting point for a critical analysis. For example, the book under review

[28] In this vein, see EVGENY MOROZOV, TO SAVE EVERYTHING, CLICK HERE: THE FOLLY OF TECHNOLOGICAL SOLUTIONISM (2014).

[29] *See, e.g.*, LAUREN BENTON, LAW AND COLONIAL CULTURES: LEGAL REGIMES IN WORLD HISTORY, 1400-1900 (2002) (about how colonial legal and religious institutions and rules co-existed and relied upon indigenous customs, social practices, institutions, religious norms and structures to maintain order).

assumes that blockchains "automagically" represent an accurate state of off-chain reality, and then speculates about what follows from that assumption. Instead of making this assumption, the authors could have asked what are the necessary preconditions of such synchronicity, and what steps the technology and real-world institutions need to take to enable the accurate on-chain representation of the world. The book discusses in some detail the question of "oracles," which make real-world facts available to blockchain applications, but fails to consider how on-chain actions are enforced to have real-world consequences. Blockchain technologies must have the capacity to enforce on-chain changes in the real world if they wish to be relevant in real-world applications, such as public records. But, like many of the issues around blockchains, this question is not intrinsic to the technology. Rather, it relates to the institutional, legal, economic, political contexts in which the technology is embedded, and which can facilitate or prevent the off-chain enforcement of on-chain alterations.[30] Going further, and looking at the question of how such synchronicity would happen, might have led the analysis in a completely different direction, one which emphasizes the mutual interdependence of law and technology, rather than antagonistic opposition between the different power regimes.

It is tempting to reduce the analysis of a complex system to a discussion of false binaries. For example, the regulatory dilemma is framed throughout the book as a balancing act between enabling innovation and societally beneficial uses (blockchain for the "good") on the one hand, and limiting illicit or criminal uses (blockchain for the "bad") on the other. This may be a relevant question for dual-use technologies, which have very specific, but highly controversial uses. Assessing the relative merits of such a technology was, for example, the task for the judges adjudicating the famous *Sony v Betamax* case,[31] who had to decide whether a copying technology was also capable of substantial noninfringing uses. But blockchains are not a typical Wassenaar-like dual-use technology[32]; rather, like a programming language, they are best seen as a general purpose technology. In fact, second generation blockchain technologies like Ethereum contain a Turing-complete programming language in their core. In addition, policymakers are not judges who have to decide case by case. Instead, they have to assess how a technology with a high potential for disruption would operate in a diverse and interdependent set of social,

[30] The book only goes so far as to acknowledge this problem at pp. 114-115 ("Garbage-in Garbage-Out").

[31] Sony Corp. of America v. Universal City Studios, Inc., 464 U.S. 417 (1984).

[32] Wassenaar Arrangement Secretariat, *List of Dual-Use Good and Technologies and Munitions List*, THE WASSENAAR ARRANGEMENT (Dec. 2017), *available at* https://www.wassenaar.org/app/uploads/2018/01/WA-DOC-17-PUB-006-Public-Docs-Vol.II-2017-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf.

economic, political contexts. The question of technology and law, we argue, is hardly reducible to the simple dichotomies of innovation vs. regulation, or good vs. bad uses.

Navigating such a landscape is mind-bogglingly difficult. It is thus important to reflect on the methods with which we compare different possibilities, or alternatives. The book uses a very US-specific analytical frame. This comment applies to both the legal and non-legal analysis. The legal discussion hardly references any non-US jurisdictions, policy approaches, regulatory solutions, or legal dilemmas. Given the global reach and popularity of the technology, this is a rather curious decision on behalf of the authors, especially given that one of them is European. The non-legal analysis also heavily relies on the law and economics approach, pioneered by US legal scholars, when it uses efficiency, transaction costs, and cost-benefit analyses to support its arguments. While such a methodological approach offers the (false) promise of a quantified, objective, empirically-grounded, and "rational" explanation as to which alternative is most desirable, or likely to succeed, it also reduces institutional, social, political, economic transformations into the monolithic dimension of economic rationality.

The future impact of blockchain technology will be visible in the changes it induces in institutions and institutional practices. We know that much of these institutional changes (or the lack thereof) happen independently of their economic rationality. They are driven by other factors: institutional inertia, history, longue durée social structures,[33] customs, irrational human behavioral traits, oddly-structured (dis)incentives, etc. There is a plethora of theoretical frames which take these factors into account, and consequently provide useful analytical tools to address the potential of blockchain technology to change social reality. Max Weber's bureaucratic theory, Foucault's analysis of power, Latour's Actor-network theory, or Bauman's liquid modernity theory, or behavioral economics, to name just a few, all offer something valuable for blockchain researchers. Yet, the book just assumes that institutional change will happen (at the extreme case, institutions will simply cease to exist) due to the irresistible force of technological decentralization and the economic efficiency that this entails. Such a reductionist approach does not seem fully justified, either theoretically, or empirically.

In short, *Blockchain and the Law* is a well-researched and courageous work, which performs the task of bringing scholarly social science blockchain research to the mainstream. Yet, as reviewers, we would have welcomed more critical distance from the subject, a more diverse and

[33] Fernand Braudel & Immanuel Wallerstein, *History and the Social Sciences: The Longue Durée*, 32 REVIEW (FERNAND BRAUDEL CENTER) 171 (2009).

inclusive scope when it comes to the legal analysis, less speculation, a bit more epistemological modesty, and better theoretical instrumentation. Still, despite its shortcomings and omissions, this book is a heroic first step in the long journey towards a better understanding of how (if ever) blockchain technology will impact our lives.