“Ruling through Technology: Politicizing Blockchain Services”

By
Guillaume Beaumier* and Kevin Kalomeni

Authors' accepted manuscript for *Review of International Political Economy*

11982 words (including references, table and abstract)

Ruling through Technology: Politicizing Blockchain Services

Abstract

Next to artificial intelligence and big data, blockchains have emerged as one of the most oft-cited technologies associated with the digital economy. Leading technology companies have recently contributed to making the technology used more widely by developing integrated blockchain offerings. The emergence of such services yet strikingly clashes with the original stated goal of the technology to remove any form of central political authority, such as the one companies behind these new services can represent. How should we then understand the embrace of blockchains by companies that this technology was notably supposed to displace? Using the concept of infrastructure from Science and Technology Studies, we argue that these companies are not merely adopting the technology but actively promoting a new assemblage of socio-technical devices to reassert their authority over how information is exchanged online. Based on a comparative analysis of the technical documentation of Ethereum and Amazon Web Services (AWS) blockchain services, we highlight how actors contributing to building digital infrastructures regulate their users' behavior by affording them different capacities and constraints. We moreover show how by pursuing its commercial interest, AWS supported a corporate form of governance historically promoted by the United States to oversee the digital economy.

Keywords: Infrastructure, Technology, Regulation, Assemblage, Blockchain, Ethereum, Amazon

Introduction

Over the last ten years, the development of blockchain technologies has been a source of great amazement and criticisms. Early supporters of cryptocurrencies were keen on maintaining that blockchain technologies were opening a new digital era. Meanwhile, many established economists and heads of international institutions warned us against falling for an economic mirage with the potential of becoming an environmental catastrophe. Despite such calls for caution, various companies now promote the use of blockchains to reduce transaction costs and make efficiency gains. Nestlé (2019), the largest food company by market capitalization, already maintains that it is using blockchain technologies to track the supply-chain of key commodities. In light of this growing interest, technology companies (e.g., Microsoft, IBM, Amazon) have developed what they call Blockchain-as-a-Service. The latter is an integrated offering allowing companies to use blockchain technologies without having to build their own. Nestlé notably uses Amazon Web Services (AWS), a subsidiary of the well-known e-commerce platform, to operate its blockchain and store information coming from its different producers and suppliers.

As it is well known, early blockchain proponents were explicitly aiming to contest contemporary political and economic orders (Golumbia, 2016; Jeong, 2013; Swartz, 2018). As Sarah Jeong describes it, the creation of the first-ever blockchain Bitcoin was in many ways a "distributed constitutional project" (2013, p. 27). The idea driving it was that central actors cannot be trusted. As it is written in the white paper introducing Bitcoin: "What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other *without the need for a trusted third party*" (Nakamoto, 2008, p. 1; emphasis added). The recent development and application of blockchains by large corporations, such as AWS mentioned above, strikingly clashes with this "libertarian techno-utopianism"

(Hütten, 2019, p. 330). Instead of undermining the role of central actors, it is used by these very actors to supposedly better govern transnational supply-chains as well as other activities involving repeated transactions among multiple actors (Campbell-Verduyn, 2018, pp. 2-3). How should we then understand these corporations' embrace of a technology that was supposed to contest their role in the global economy?

In this paper, we argue that the rise of private blockchain services represents an attempt by the companies behind them at establishing socio-technical systems to assert their authority over new digital transactions enabled by blockchains. As previous international political economy scholars have emphasized (Bernards & Campbell-Verduyn, 2019; Denardis, 2012; Deibert, 2003), technological changes are not merely about productivity gains but also power and control. By designing the technical features of new technologies, private companies aim to define what their end-users will be able to do. This represents a regulatory activity through which they attempt to promote their economic ideas and market logic (De Filippi & Wright, 2018; Jeong, 2013; Lessig, 1999; Porter, 2003). Instead of occurring through social, legal or market pressures, it primarily results from the continuous adaptation of infrastructures that can determine users' "affordances and constraints" (Benkler, 2011a, p. 722).

As just mentioned, early blockchain creator(s) were trying to challenge the global economic system. Instead of merely lobbying public authorities for legal changes, they creatively assembled preexisting technologies to develop an infrastructure to define how information can be exchanged online. Over time, new technologies can importantly be re-appropriated or re-regulated. Just as laws can be amended or adapted, any assemblage of material and ideational elements forming a specific infrastructure can be changed to remove or create new constraints for its users. If

technologies can regulate the behavior of their users, the latter can also re-regulate the former. With that in mind, all users are not equal in that process.

In this paper, we specifically highlight the key influence of private actors maintaining and connecting smaller socio-technical systems to broader infrastructures in the global economy. As they continuously invest resources and shape the technical systems that other users work through, they can embed their ideas in it and regulate other users accordingly. This does not prevent future users to challenge their authority, yet they will have to work through the infrastructure that they have established or to compete with it by developing a new one, which will require significant ideational and material resources. Through focusing on AWS, we moreover highlight how by creating a blockchain infrastructure aimed at ensuring its own central authority and extracting economic rents it supported a corporate form of governance preferred by the United States to oversee the digital economy.

Meanwhile, we point out that despite embracing a similar "libertarian techno-utopianism" to early Blockchain developers, Ethereum did not entirely escape centralization forces. By maintaining and connecting its blockchains services with broader socio-technical infrastructures, Vitalik Buterin, one of Ethereum's co-founders, and the Ethereum Foundation act as *de facto* regulators. In line with other research that emphasized the centralization tendencies in the Bitcoin infrastructure (Campbell-Verduyn & Goguen, 2019; Swartz, 2018), this points to the simple fact that complete decentralization remains a utopia. If the development of new blockchains can be used to challenge the centrality of some economic actors, the re-ordering of relations that they promote will often result in supporting new tendencies towards power centralization (Schneider, 2019).

In making these arguments, our work contributes to the current literature in three important ways. First, we build on recent scholarship enjoining international political economy (IPE) scholars to give greater attention to infrastructures to understand "questions of authority, governance and power" in the global economy (Bernards & Campbell-Verduyn, 2019, p. 775; see also Braun, 2020). Here, we more specifically highlight how actors adapting small-scale technical systems can have lasting effects on the global economy. We likened this to a regulatory form of power through which they shape other users' behavior by again setting out specific "affordances and constraints" (Benkler, 2011, p. 722).

Second, we broaden the study of blockchain technologies by looking at how they are increasingly offered as integrated services outside the financial realm. Up to now, most of the literature has remained primarily focused on the case of Bitcoin and few other prominent financial applications of blockchains (Campbell-Verduyn, 2018; Golumbia, 2016; Jeong, 2013; Rodima-Taylor & Grimes, 2019; Reinsberg, 2019; Rosales, 2019; Swartz, 2018). Blockchain technologies are, however, increasingly used to exchange other types of valuable information, like property rights, and build so-called "smart contracts" offering new avenues for private actors to control how value is created and shared. By explaining how blockchains are used for these additional purposes, we refine the current understanding of how this technology might impact the global economy in the years to come.

Third, and finally, we provide a first comprehensive list of the technical characteristics of blockchain technologies. Different studies have mentioned that blockchains are based on encryption, peer-to-peer and time-stamping technologies (Campbell-Verduyn, 2018; Narayanan & Clark, 2017). We show how these, and other technologies, are combined to form six interrelated technical characteristics, which we use to explain how they can be adapted to fit different political-

economic ideas. This significantly allows us to go past the simple centralization/decentralization dichotomy and point out the multiple socio-technical choices involved in maintaining and connecting blockchains to broader infrastructures in the global economy.

The rest of this paper is divided in four sections. In the first section, we review recent strands of literature standing at the crossroad of international political economy and science and technology studies (STS). Based on this, we explain the value of looking at the power of blockchains and actors maintaining them through an infrastructural lens, and further define the key concepts of infrastructure and assemblage. The second section offers a brief presentation of the evolution of blockchain technologies since the inception of bitcoin and how we came to our six technical characteristics. The third section presents a comparison of Ethereum and AWS' blockchain infrastructures based on these six technical characteristics and their connections to their respective economic ideas and interests. The fourth section finally proceeds with an analysis of how each used its position in their blockchain infrastructure to regulate other users.

Regulating through Infrastructural Change

Infrastructures are colloquially understood as "large-scale technical systems" (Bernards & Campbell-Verduyn, 2019, p. 776). This is broadly meant to define many systems that exist in the background, are often taken for granted and allow for all sorts of activities to take place (Edwards et al., 2009; Star, 1999). Traditional examples include electrical grids, water systems, information networks and railway networks. More than simply understanding them as *technical* systems, we here follow recent work in international political economy integrating insights of Science and Technology Studies (STS) and considering them as "contextualized relations" between non-human objects and human practices (Bernards & Campbell-Verduyn, 2019, p. 777; see also Karasti et al.,

2016). In other words, we understand infrastructures as *assemblages* of both material and ideational elements. The concept of assemblage is here used to describe how through their combination, and as a whole, these material and ideational elements become stable and enable new activities to take place, which represents an exercise of power (Latour, 1991). While contingent and open to change, these assemblages can indeed shape the everyday actions of those using the technology, and thereby either reinforce or contest preexisting power relations. In the context of the present study, it will notably be shown how they can produce different models of governance to oversee the digital economy.

To give a concrete example, we can consider the Internet infrastructure. The latter is evidently composed of a wide variety of interconnected technical devices that include such things as computers, submarine cables, satellites, data centres and various software. All these technical artefacts importantly only do anything when assembled with specific human policies and practices. One of the main technical components of the Internet is more precisely its domain name system (DNS). The latter is the technical protocol devised by early Internet developers to attribute an individual name (e.g. "Amazon.com") and related IP address (e.g. 172.15.254.1) to computers all around the world. While seemingly trivial, the creation of these unique identifiers for each computer is actually what allows them to communicate electronically with each other. It is equivalent to the mailing address system without which no letters could ever reach its recipients. It technically connects the different devices that form what we take as the Internet. More than a technical protocol, though, it reflects specific policy choices that have been made over the years.

The relations between these social and technical aspects "become [particularly] visible upon breakdown" (Pipek & Wulf, 2009, p. 454), that is when tensions arise, and the normal working of the system is being questioned. This can notably be seen in the early days of the Internet. As

tensions arose between the original community of developers and the new company in charge of maintaining the root server of the DNS, Jon Postel, an academic from UCLA, attempted to give himself the authority over it by e-mailing operators of the different servers and requesting them to recognize him as the new root (Goldsmith & Wu, 2006, p. 29). As they all agreed to do so, he gained control over the root of the Internet for a brief moment. Following clear indications that his continuing interference with the basic infrastructure of the Internet could be considered a criminal offense, he gave back the control over the DNS to the company the American government had tasked with maintaining it. These two competing assemblages of socio-technical devices interestingly aimed to promote contrasting forms of Internet governance. In the first assemblage, the recognition by a small group of scholars that the computer of Jon Postel was the authoritative root of the Internet was notably based on the idea that the Internet should be managed collaboratively and not in the hands of a for-profit organization. In the second assemblage, the United States specifically favored having a private company as the main point of control in the Internet infrastructure. As it will be discussed at greater length in the next section with regards to the development of the blockchain infrastructure of AWS, this reflects a situation where the interest of a private company to accrue profits supports the interest of the American government to work with a clear and identifiable intermediary rather than a distributed network of actors.

This story of the early fight over the root Internet moreover shows how infrastructures always work based on multiple interactions between technical devices and human practices. While the technical working of the DNS did not *per se* change, the decision by human operators to accept Jon Postel's request had the effect to change momentarily the infrastructure of the Internet. This was moreover only possible by the technical nature of the DNS, which relied on local servers recognizing one root. This crucially points to the co-constitution of the technical devices and social

relations that form an infrastructure. Rather than being one of the two that straightforwardly control the other, it is their joint interactions that enable any actions. As Nick Bernards and Malcolm Campbell-Verduyn put it, a focus on infrastructure as socio-technical systems allows to bridge the "material and ideational" as well as the "technical and political" gap (2019, pp. 777-780). This significantly helps avoid recurrent tendencies towards technological determinism in IPE (McCarthy, 2013). Taking infrastructures as socio-technical systems both recognizes that any actor has to deal with the material reality of the infrastructure and the latter's effect are always contingent on the ideas being promoted at a specific point in time.

This specific approach to the study of infrastructure moreover allows for a more nuanced understanding of agency. While debates over the "structure–agent problem" continue to divide IPE scholars, it is often much less controversial that it is *human* agents that act (Leese & Hoijtink, 2019, p. 10). In similar fashion to deterministic reading of technology, they (un)consciously bracket "the question [of] who can act" and implicitly assume that only conscious actors can produce changes in the real-world (Leese & Hoijtink, 2019, p. 11). This fails to capture the many unpredicted ways in which the material world affects human actions and even sometimes determines its outcomes.

This can again be illustrated by looking at the governance of the Internet infrastructure and one of its most recent debates following the adoption of the General Data Protection Regulation (GDPR) by the European Union. As previously explained, the DNS connects all IP addresses to domain names and practically allows the Internet to work as it does. This requires domain name registrars to collect information on who wants to create a website and attribute them single identifier. Early on, it was decided that this information would be made available through the public database WHOIS to ensure that it would always be possible to identify who was behind a specific webpage.

As Samantha Bradshaw and Laura Denardis point out, this choice was originally made when the Internet was still an academic project connecting "a small number of (trusted) users" (2019, p. 18). This specific policy however came to clash with the GDPR and its principle of data minimization proscribing large distribution of personal data such as those found in the WHOIS database. To resolve this, the GDPR rules had to be interpreted and adapted in the specific context of the Internet technical protocols. While waiting to find a final solution, ICANN, the main entity today overseeing the DNS, put in place temporary specifications requirements allowing registrars to collect registration data and controlling access to it in respect of the GDPR.

This example shows that human actions will unsurprisingly be shaped by their material environment. This could lead some to again argue that what matters is understanding the intent of human agents and how it is mediated by non-human objects. We however believe that a more fruitful approach is to consider agency as the "product of [their] interaction" (Leese & Hoijtink, 2019, p. 3). This effectively makes the question of agency an empirical rather than an ontological one (Braun et al., 2019). Instead of automatically attributing primacy to humans in producing change, it recognizes how agency is actually contingent on the specific connections that will exist between humans and material devices at specific points in time and place. This closely aligns to various works subsumed under the heading of New Materialism (Connolly, 2013). In the specific study of the evolution of infrastructures as socio-technical systems, it broadly means that we see agency as the result of the very interactions between the actors, ideas and material components forming an infrastructure.

In the rest of this paper, we focus on a very specific nexus of the three in building small-scale socio-technical systems. We specifically look at how actors in charge of maintaining and connecting blockchain services can influence their users' behaviour through their interactions with

the technical components forming a blockchain and connection with broader infrastructures. Up to now, the concept of infrastructure was qualified to mean systems made of socio-technical devices. At the same time, it was still presented as mainly representing large systems as the example of the Internet infrastructure could let think. Following the relational view of infrastructure promoted by Nick Bernards and Malcolm Campbell-Verduyn (2019, p. 779), we would yet suggest that it is best to understand such large infrastructure as themselves composed of smaller infrastructures. As Volkmar Pipek and Volker Wulf explains, this embeddedness of infrastructures is the result of a continuous process where new "infrastructures are plugged in other infrastructures" (2009, p. 454). Far from starting from nothing, new socio-technical systems recombine preexisting socio-technical devices and connect themselves to other preexisting infrastructures. The process of infrastructural change is thus often one of "layering" rather than pure competition or displacement (Rodima-Taylor & Grimes, 2019, p. 847). New socio-technical systems will be developed to work with the broader socio-technical environment in place. This is again perfectly encapsulated in the Internet infrastructure, which is presented as being made of multiple interconnected layers (Fransman, 2016) and a network of networks. To describe this reality, Pipek and Wulf aptly talk of *infrastructuring* to highlight the continuous process of connecting socio-technical systems.

This also helps escape one more dichotomy often found in the study of material objects: developer–user. As expressed early on by Langdon Winner (1980), it has been common for those interested in the politics of technical artifacts to point at their supposed moment of constitution. The argument was that by bringing out the social elements of that specific moment, one would in effect be able to uncover the politics behind technological change. This ends up offering an essentialist view of technology as it broadly assumes that once its original designer has ascribed it an essence, it will

never change. The technical then becomes irrelevant, and what matters is the original intent of a technology's creator(s). The argument developed here according to which new socio-technical systems continuously build on preexisting infrastructures instead imply that the development of a technology always results from the assemblage "of multiple old and new devices" (Bernards & Campbell-Verduyn, 2019, p. 777), a process through which an actor is both constrained by the socio-technical system in place and actively trying to shape it. These specific moments can be viewed as "points of infrastructure" (Pipek & Wulf, 2009, p. 458) that occur when preexisting infrastructures meet the "creative" actions of actors developing a new technology. This can importantly occur at various levels. Daivi Rodima-Taylor and William Grimes notably show how new remittance infrastructures will continuously depend on "the role of local entrepreneurs and social networks solving the 'last mile' problem" (2019, p. 842).

Yet not all actors are equal in that infrastructuring process and can position themselves at these crucial points of infrastructure. Having access to both significant material and social resources will be crucial. It will in effect determine their capacity for doing the mundane work of maintaining the infrastructure and bringing others to use it. Hereafter, we argue that those that however successfully do so will have the opportunity to embed their ideas in the infrastructure and regulate the behaviour of other users accordingly. If again, they are themselves limited by the existing infrastructure that they have to connect themselves to and what others will decide to do with their own infrastructure 'on the ground' (i.e., at other layers of application), their own infrastructural work will effectively regulate the activity of others.

The regulating power of technologies is not new. In the context of the digital economy, Lawrence Lessig famously coined the expression *code is law* (1999). By the latter, he meant that by giving specific instructions to computer programs, technical engineers act as regulators, setting out what

practices would be acceptable in the digital environment. Next to social, market or legal pressures, this represents a fourth and "architectural" mode of regulation (De Filippi & Wright, 2019, p. 174). By designing the digital infrastructures, they define what others can do by attributing different "affordances and constraints" to each and every one active in it (Benkler, 2011a, p. 722). To make a parallel to the physical world, they act similarly to architects and urban designers that regulate our daily behaviors through the design of physical infrastructures (Winner, 1980). The infrastructural lens that we adopt importantly leads us to approach this regulating power in a relational or interactive fashion. As opposed to Lessig (1999) who portrayed technical engineers as regulating on the equivalent to a blank page, we consider that it is the active process of connecting new socio-technical system to preexisting infrastructures that represent the regulatory activity. This is in line with our understanding of agency as resulting from the combination of the human agents and their connections with technical devices. Once again, this means that the process of regulation, just as the one of infrastructuring, will never be complete. Other users will continuously attempt to re-regulate a new technology. It reflects the ever-present "process of infrastructural contention" (Edwards et al., 2009, p. 372). This will however require them to spend resources to propose a new assemblage of the socio-technical devices connecting multiple infrastructures together.

The current development of blockchain technologies illustrate this dynamic. By proposing a new technology, early developers behind Bitcoin effectively innovated by assembling together preexisting technologies and actively "piggybacking" on the Internet infrastructure (De Filippi & Wright, 2019, p. 46; see also Narayanan & Clark, 2017). Through this work, they gave specific capacities and roles to those wishing to exchange value outside of the financial realm. Since then, other actors have worked to repurpose and re-regulate blockchain technologies. In this paper, we

specifically review two of such attempts by Ethereum and AWS. Through a comparison of the infrastructures that they each built, we moreover show that while the former regulates according to a similar libertarian ideal to early blockchain developers, the latter instead supports a corporate form of governance promoted by the American government since the early days of the digital economy. Before turning to this analysis, the next section will introduce at greater length what are blockchains, how both Ethereum and AWS differ from the early formulation of the technology, and how we came to the six technical characteristics that we will use to compare them.

From Bitcoin to Blockchain-as-a-Service

The origins of blockchains remain to this day imbued with a dose of mystery. While actually never mentioning it by name, the idea of a blockchain was famously first enunciated in the Bitcoin white paper published by the unknown developer(s) behind the alias Satoshi Nakamoto. Since the inception of Bitcoin in 2009, multiple works have traced the roots of this new technology and offered an increasingly detailed account of what blockchains are and where they come from (Brunton, 2019; Campbell-Verduyn, 2018; Narayanan & Clark, 2017; Swartz, 2018). Technically, blockchains are digital ledgers which aim to securely and anonymously record the exchange of value between various individuals without the need of a trusted third party. Financial services traditionally rely on the presence of a trusted intermediary to confirm the validity of economic transactions and keep a valid record of them. Most prominently, banks play this role every day when consumers exchange money for various products and services. Without them, the risk is that malicious actors try to duplicate financial information and use it for multiple transactions. A situation where someone would basically use the same money multiple times.

To solve this "double-payment" issue without relying on trusted intermediaries, blockchain technologies primarily make use of recent encryption and time-stamping technologies (Campbell-Verduyn, 2018; Narayanan & Clark, 2017). In short, economic transactions are validated by a network of computers solving complex mathematical problems, which are then recorded as part of a "block" of data. When the block of data reaches a certain size of information (e.g., 1000 transactions), it is joined to previous blocks to form a chain of blocks ("blockchain"). Time-stamping technologies are then used to secure the entire chain of information by making it impossible to change one block without having to change the entire blockchain, which would require tremendous computing power. One change would in effect require redoing all the complex mathematical problems for all the blocks that came after the one attempted to be changed. Finally, the security of the blockchain is supposed to come from its distribution among all its participants. The actual and valid chain of blocks will be the one respecting a pre-defined consensus requirement. The most common one is that more than half of the computers part of the network of participants validate a transaction before it can be added to the blockchain. This is technically called the "Proof of Work" system and means that one user cannot individually change the blockchain because it would require to have at least more computing power than half of all users to make its modifications valid.

While the first ever blockchain created was also the first ever cryptocurrency (i.e., Bitcoin), it is important to distinguish the function of blockchains as digital ledgers from the monetary system promoted by cryptocurrencies. The latter are certainly related as they were both created at the same time, but blockchains have wider applications than the sole transfer of financial information. Since the inception of Bitcoin, blockchain technologies have been applied to an increasingly diverse set of economic activity and exchange various types of valuable information (Swan, 2015). Property

rights are one such example (Garrod, 2019). Instead of relying on notaries or other legal representatives, blockchain technologies can be used to record property rights. ‘Smart contracts’ are another recent application of blockchain technologies, allowing value to be automatically transferred when specific conditions are met. Insurance payments are one important use case for that type of application. Another exemplified by the case of Nestlé briefly presented in introduction, blockchains can also be used to record and transfer proprietary information along supply-chains.

All these different applications progressively led to the development of multiple blockchain projects beyond the original Bitcoin. The so-called Big Four of consulting firms (i.e., KPMG, PwC, Deloitte, and EY) “increasingly promote blockchains as means of improving the effectiveness of supply-chain governance” (Bernards et al., 2020, p. 524). Apart from the multiplication of cryptocurrencies, there are now various initiatives that build and manage blockchains specifically for the operation of smart contracts. In corporate circles, it notably includes the recent development of Blockchain-as-a-Service (BaaS). The latter is an integrated offering through which large technology companies (e.g., Microsoft, IBM, Amazon) manage a blockchain infrastructure to be used by other companies. More than simply representing a new service, the work of these companies actively aims to re-regulate the technology to fit their own political-economic agenda. By maintaining and connecting different socio-technical devices together and with the broader infrastructures, they define what their users can do. In the next section, we demonstrate this process of regulating through infrastructural change by comparing the blockchain infrastructure built by Ethereum and AWS. We selected these two cases for their broad significance in the blockchain ecosystem and as representing two ideal-types.

Ethereum is the second-biggest "cryptocurrency"[1] (behind Bitcoin) created by early members of the blockchain community (Buterin, 2013). Many new uses of blockchains, including smart contracts, were first put into practice by Ethereum (Swan, 2015). The prominence of Ethereum is such that various private companies currently use it to develop their own blockchain services. While generally not included as a provider of Blockchain services, it acts quite similarly by allowing individuals or organizations to program and execute smart contracts using its infrastructure (Hutten, 2019; Swan, 2015).

While differing from Bitcoin and itself representing an attempt at re-regulating blockchains, it moreover integrates many of the original beliefs of the cypherpunk and crypto-anarchy communities. Without going into too many details about these two interconnected and evolving communities that have been identified at the origins of Bitcoin (Swartz, 2018), it can be broadly said that both follow the work of American anarcho-capitalist thinkers (Friedman, 1973; Rothbard, 1970) in taking the concept of private property as absolute. For them, any entity attempting to subdue private property is basically restricting the proper functioning of the *natural* free market and, as such, an illegitimate source of authority that needs to be contested. States and large corporations are in that respect the usual suspects that they aim to upset and replace as they see them as colluding together to build monopoly privileges. These very ideas were at the heart of the development of Ethereum, which according to one of its co-founders, Vitalik Buterin, notably aimed to reorganize ownership rights through smart contracts. As he explained, access to one's apartment could be tied to an automatic payment to his/her landlord or bank, and failure to pay would alternatively result in being locked out of one's home (Garrod, 2019, p. 605). These ideas

[1] The word cryptocurrency continues to be used to describe most projects applying Blockchains even though they do not all aim at creating a global currency like Bitcoin.

famously came to life in The DAO (an acronym for decentralized autonomous organization), a short-lived crowdfunded venture launched on the Ethereum blockchain and that aimed to automate the process of raising and investing money. The exploitation by hackers of technical vulnerabilities leading them to drain almost a third of the money that it had raised however led it to have to forgo its own rules and eventually its demise (Hutten, 2019). Despite this unfortunate result, the Ethereum blockchain continues to be used by various projects animated by this idea of building decentralized autonomous organization.

In comparison, AWS represents an example of a traditional private company offering a blockchain service. As of now, the three most oft-cited companies devising such services are AWS, IBM, and Microsoft[2]. The reason behind the choice to focus on AWS is twofold. First, AWS is by far the global leader in cloud computing services and can easily attract other prominent companies – like Nestlé as previously mentioned – to use its services,. While smaller start-ups have recently been working on developing and offering blockchain services, AWS basically has the capacity to affect more end-users by combining its blockchain offering with its cloud services. Second, its own blockchain service builds on the technology of the Hyperledger Fabric open-source project created by a consortium of other large corporations, including IBM, Intel and J.P. Morgan (AWS, 2020a, p. 1). As such, it closely approximates the services being developed by its competitors and we consider it to be broadly representative of what corporate attempts at building blockchain infrastructures look like.

Concomitantly, AWS epitomizes the corporate form of governance despised by Ethereum and other early blockchain projects. As the next section will detail at greater length, its desire to accrue

[2] For other prominent examples, see inter alia: https://news.bitcoin.com/7-of-the-worlds-largest-blockchain-as-a-service-enterprises/.

economic rents led it to continuously aim to position itself as the central authority in the blockchain infrastructure it has been building and become a prime collaborator for states to regulate how value is being exchanged online. By providing a clear intermediary to work with, large corporations such as AWS can in effect help states achieve their regulatory aims more efficiently (Braithwaite, 2008; Mikler, 2018). In the digital environment, the United States has for long championed this specific form of governance as the presence of some of the largest technology companies in the world on its territory helps it extend its regulatory influence in other jurisdictions and access data it could have never collected without their help (Zuboff, 2019). This type of collaboration between the American government and large technology companies can also be seen when digital platforms like Google remove material supposedly infringing intellectual property rights (Carthwright, 2021, p. 155), online payment services stop allowing their services to be used by companies infringing American law (Tusikov, 2017, p. 87-88; Benkler, 2011b, p. 341), or Internet service providers share large amounts of information about their users to the American government (Bauman et al., 2014, p. 123).

This should importantly not be taken to mean that the relation between the American government and large technology corporations like AWS has always been harmonious. In 2015, Apple famously refused to provide access to the iPhone of the San Bernardino shooter to the FBI and, in 2018, Google put an end to a lucrative partnership with the Pentagon following pressures from its employees who considered the project to go against the company ethical principles. Uber is moreover a prominent example of a technology company that in many ways build its business model around a challenge to preexisting state regulations (Barry and Pollman, 2016). Tensions between the interests of private companies and public regulations have thus emerged from time to time.

Having said that, both sides clearly tend to recognize the benefits to work with the other. Again, the American government sees an opportunity in working with these companies to exert its influence globally and leverage their data collection capacities for its surveillance interest. Meanwhile, these same companies regularly look for the American government to help them entrench their position in the digital marketplace. Once disruptors will often see quite positively the adoption of "regulations they know they will easily satisfy, but that small competitors will not be able to manage" (Braithwaite, 2008, p. 20). Internationally, they will more often than not rely on the American government to defend their business interests as we could see from recent debates around the adoption of data localization laws that would effectively raise their cost of doing business by requiring them to build data centres in every country adopting them. As the next section will show, by encoding its commercial interest in its blockchain service, AWS upheld this corporate form of governance that early blockchain users, like Ethereum, had hoped to replace.

To compare how Ethereum and AWS each attempted to regulate their users through the development of their respective blockchain infrastructure, we identified six basic technical characteristics where they assembled different socio-technical devices together and connected with broader infrastructures. These are (1) credentials, (2) identification, (3) price system, (4) consensus system, (5) data storage and (6) compatibility. As previously noted, it is generally recognized that blockchains innovated by bringing together time-stamping and encryption technologies. It is in effect by assembling these different technologies and adapting them to fit in preexisting infrastructures that actors, like Ethereum and AWS, can create blockchains with contrasting attributes for each of these six characteristics and promote different regulatory aims. While all discussed in the literature (Campbell-Verduyn, 2018; Gerard, 2017; Narayanan & Clark, 2017; Swan, 2015), no other work has up to now provided a clear and comprehensive list of these

technical characteristics. Primavera De Filippi and Aaron Wright probably came the closest to it in their recent book *Blockchain and the Law* (2019, Ch. 2), yet they indiscriminately mix expected outcomes (e.g., disintermediation) with actual technical characteristics (e.g., consensus system). They moreover provide characteristics (e.g., pseudonymity) that only define some blockchains and that we broaden (e.g., identification) to highlight how multiple blockchains actually differ. With this in mind, we defined the six characteristics above-mentioned based on previous insights found in the literature and an inductive analysis of the main technical documentation of Ethereum and AWS' blockchains. The latter included "management guide", "white papers" and "technical guidelines", which were used by these two actors to present their respective technologies and explain their technical characteristics to their users. The next section will now compare how Ethereum and AWS differ in terms each of these six characteristics and how they relate to different political-economic ideas.

Ethereum and AWS: Two Socio-Technical Infrastructures

In line with their different political-economic ideas, Ethereum and AWS developed strikingly different blockchain infrastructures. While Ethereum tries to eliminate most intermediaries in line with its crypto-anarchist and cypherpunk ethos (Swartz, 2018), AWS continuously places corporate actors at the heart of its blockchain infrastructure. Table 1 summarizes how each differs in terms of the six technical characteristics previously introduced. We hereafter discuss how these discrepancies reflect a unique combination of socio-technical devices and produce different regulations. If presented separately, it should be clear that it is however through the combination

of all of them that a blockchain can function. This will be made clear by the multiple connections drawn between them in the analysis.

Insert Table 1

Credentials

The first technical characteristic of a blockchain infrastructure is its credential system, which determines who can access it. Many digital infrastructures nowadays operate a verification system that checks the identity of anyone wishing to take part in them. Only those with valid credentials are allowed to join and contribute to these infrastructures. Different credentials often coexist and afford varying capacities to the distinct categories of users (e.g., consumers, code developers).

One of the original innovations brought by early blockchain technologies, and notably Ethereum, was the rejection of this traditional credential system where one actor affords different permissions to others. No participants can refuse another to join the network of actors, nor can they give specific permission to determine what some users can do or see. In effect, anyone can join it in the capacity they want. It can be to develop new applications and services, use its computing power to approve transactions or even join its community of developers. The only real limitation is that a participant will need to have the material capacity to connect itself to the Ethereum network and the knowledge to do so. Any interested party can otherwise download Ethereum client portal, follow the documentation freely available, and connect to its network (Ethereum, 2017). As opposed to AWS, Ethereum thus represents a permissionless or *public* blockchain.

In contrast, AWS follows a permissioned approach, which occurs at multiple levels. First, the creator of a new blockchain network (e.g., a bank or food company) must define a "voting policy" determining how new members can join it (AWS, 2020a, p. 4). Only those who will be approved

following the rules of this voting policy will be given the permission to join the network and contribute to the blockchain by adding and/or validating transactions. The same voting policy can importantly be used later on to exclude some members (AWS, 2020a, p. 36). Second, and as discussed at greater length below, blockchains managed by AWS do not function with one ledger as original blockchains would, but multiple ones. In effect, "a ledger exists in the scope of a channel" that can include all members or only few of them (AWS, 2020a, p. 19). This means that instead of having one decentralized ledger accessible to all members, there are multiple private ledgers to which members need to be given the permission to join. Otherwise, they only have a partial view of the transaction's happening on the blockchain network. Third, all members joining an AWS' blockchain network will start by internally specifying an "administrator" of their account (AWS, 2020a, p. 57). The latter is in charge to determine who from their own organizations can do what on the blockchain by giving them different "credentials and permissions" (AWS, 2020a, p. 60).

This first disparity in the technical characteristics of the blockchain services of Ethereum and AWS importantly reflects their different assemblage of socio-technical devices. Ethereum basically rejects that one or few users should act as the gatekeepers to create security. It does not maintain any credential requirements. The security and integrity are primarily maintained by establishing economic incentives and a consensus system discussed at greater length below. Meanwhile, AWS aims to devise a blockchain infrastructure where some of its users retain the capacity to control who can take part in it. This interestingly leads it to argue that it provides a more secure environment than public blockchains like Ethereum. This yet means that the initiator of a blockchain network maintained by AWS has a significant say over who can join its network. At

one extreme, it could even decide to have a veto power and requires that all new members need its approval to join the blockchain network.

Identification

A second key technical characteristics of blockchains is how they identify their users. Ethereum here functions with public addresses that act as pseudonyms for its users (Ethereum, 2017, p. 37). Anyone can thus follow what others do on the blockchain, but they cannot know who they actually are. Even non-Ethereum users can go online and download the list of all transactions and involved users. The use of pseudonyms aims to ensure that the privacy of all users is guaranteed as original cypherpunks hoped for.

In contrast, and in line with its permissioned credential system, AWS relies on the clear identification of all participants. When voting on the addition of new members, existing ones will know their identity and their future identifier (AWS, 2020a, p. 52). Internally, all members' organizations also operate an identity and access management system through which they manage the identity of all their users and use this information to decide what actions they can perform (AWS, 2020a, p. 60). As clearly indicated in AWS' Management Guide:

> An [Identity and Access Management] administrator can use policies to specify who has access to AWS resources, and what actions they can perform on those resources. […] In other words, by default, users can do nothing, not even change their own password. To give a user permission to do something, an administrator must attach a permission policy to a user (AWS, 2020a, 63).

Interestingly, AWS actually maintains to be more privacy-friendly than Ethereum (AWS, 2019). This claim importantly has to be evaluated by looking at what information is actually kept private and from whom. In the case of blockchains managed by AWS, the identity of all members of the blockchain network is kept private from the broad public but is known by the other members of

the network. Similarly, transaction information is only available to members of the blockchain or of a subset of members when it is part of a private channel. In short, AWS aims to ensure the security of its service by maintaining a database of its users' identity that each will have access to depending on their specific credentials. In contrast, Ethereum protects the privacy of its users through the use cryptographic technology that allows to link a public address (or identifier) to a private key.

Pricing system

A third essential technical characteristic of blockchain infrastructures is their pricing system. Original public blockchains such as Ethereum integrate a dynamic market logic to establish what contributors will pay to use its blockchain service. When a user wants to execute a specific operation using Ethereum, like implementing a smart contract or validating a transaction, its request will contain information about the amount of "gas" it is willing to spend (Buterin, 2013, p. 14). The gas is the fee for which another user will be ready to run the computer code to complete the requested operation and validate an operation (Ethereum, 2017, p. 49). This is a voluntary process and "the price of gas is decided by the miners, who can refuse to process a transaction with a lower gas price than their minimum limit" (Ethereum, 2017, p. 68).

In other words, Ethereum uses computer code to act as a kind of *free market* regulator and attempt to create an unmediated market as envisioned by crypto-anarchists (Swartz, 2018). Prices are designed to fluctuate depending on changes in supply and demand. The permissionless nature of Ethereum moreover plays a key role in ensuring the competitive nature of this system. As anyone can decide to lend its computing power, it supposedly ensures that a competitive process will progressively drive out those with higher computing costs and attract those with lower ones. In practice, material and energy costs are important barriers to entry and limit the participation of

some actors, which can end up creating market concentration as notably seen in the case of Bitcoin (Campbell-Verduyn & Goguen, 2019). This highlights that despite originally aiming to be decentralized, a blockchain infrastructure might well evolve in the opposite direction based on the actions of its users.

In comparison, AWS adopts a fixed prices approach that works through traditional financial intermediaries. In short, it sets in advance a list of fees that its users have to pay based on their activities on the blockchain network (AWS, 2020b). These fees are fixed until AWS revises them. Each new transaction or information validated and saved on the blockchain costs the same to its users based on AWS' commercial strategy. While competition with other providers of blockchain as a service should limit its capacity to act as it wants, the limited compatibility of its services discussed below also means that its clients cannot easily move their blockchain network to other companies maintaining blockchain infrastructures and creates an opportunity for rent-seeking.

Consensus

The fourth fundamental technical characteristic of any blockchain infrastructure is how transactions or operations for a smart contract are validated. Again, this is more commonly known as the consensus system which most often foresees that half the participants need to agree to officially record a transaction or operation on a blockchain. This "Proof of Work" (PoW) consensus system is, however, only one technical approach and different blockchain services can use different ones. Because of the significant amount of energy that a PoW consensus system uses (Gerard, 2017, p. 15), different blockchains are now experimenting with what they call a "Proof of Stake" system where transactions are validated by participants that have agreed to put at stake a minimal amount of money or cryptocurrency (Hsieh and al., 2018, p. 56). If a transaction would

be found to be wrong or malicious, the participant that approved it would lose its stake, making it costly to cheat.

While currently transitioning towards the latter mechanism, Ethereum still follows a PoW consensus system and forces all users sharing their computing power to compete to add as quickly as possible new transactions to the blockchain. The fact that each addition of blocks of data is the result of a competitive process is in effect the key element that assures that the data validation process is effectively decentralized and secure. There is no central authority that has to power to validate transactions or block them. Reversing what has been added to the blockchain would again require that more than half of the participants turn rogue or that one actor ends up controlling the majority of the computing power within the network. As just mentioned, the rise in material and energy costs could yet lead to greater market concentration.

In the case of AWS, members of one of its managed blockchain are free to choose the consensus system that they want to operate (AWS, 2020a, p. 4). In practice, each creator of a "channel" on a blockchain managed by AWS has to define an "endorsement policy" indicating which or how many members need to validate a transaction or operation to be recorded on the blockchain. In AWS *Management guide*, it is outlined that only two organizations could notably validate a transaction: "The channel creator (org1) runs the following command to instantiate the chain code with an endorsement policy that requires both org1 and org2 to endorse all transactions" (AWS, 2020a, p. 30). Through its code, AWS once again gives the main authority over the blockchain that it manages to their initiators. While the latter could hypothetically decide to operate a PoW consensus system, the example given by AWS highlights that they would probably not. There is even an economic disincentive to do so as it would require renting out and paying for more

computing power than by relying on a limited number of users ("validators") with the capacity to approve transactions on the blockchain.

Data storage

A fifth technical characteristic when looking to a blockchain infrastructure is how data is stored. As explained in the previous section, the primary purpose of a blockchain is to record an exchange of information. Ethereum here aims to be a distributed network, which means that all its participants could have a copy of the information recorded on the blockchain. This is supposed to ensure that everyone can equally monitor what transactions are being approved and added on the blockchain, rather than one central entity. To ensure this, it only allows a limited amount of information to be stored in each block. It reflects the fear of its founder in creating an unequal system between nodes that could encourage collusion between the most powerful one:

> "The problem with such a large blockchain size is centralization risk. If the blockchain size increases to, say, 100 TB, then the likely scenario would be that only a very small number of large businesses would run full nodes, […] In such a situation, there arises the potential concern that the full nodes could band together, and all agree to cheat in some profitable fashion […]" (Buterin, 2013, p. 33).

In other words, Ethereum aims at preventing that few actors with superior material capacity (i.e., large corporations) end up dominating the network by technically limiting the storage capacity needed to record transactions on the blockchain. By putting a cap on the advantage of more powerful computers, Ethereum hopes that a wide range of users retains the capacity to operate verification nodes and maintain a copy of the entire blockchain.

As a corporate entity, AWS meanwhile rents its storage capacity to its clients with none or very little size constraints (AWS, 2020a, p. 42). Everyone participating in a blockchain managed by AWS simply decides how much storage they need to run their part of the chain. The only real

limitation one is the price of the data storage that a user is willing to pay to enjoy its service. Again, this and the possibility for users of AWS' managed blockchain services to build private channels means that not all participants will necessarily have access to the entire blockchain. As opposed to the distributed model put forward by Ethereum, only some users could have access to the entire blockchain and most would probably only have information on the part saved on the private channel that they have access to.

Compatibility

The sixth technical characteristic of blockchain infrastructures is their compatibility or how easily their users can use the data recorded on the blockchain with other technical systems. Ethereum is fully interoperable with other blockchains and socio-technical systems. As specified by its founder, Ethereum technology is "Turing complete", meaning that it accepts all types of programming language (Buterin, 2013, p. 13). Guidelines to run nodes are easily available online without having to pay the Ethereum foundation itself or any other entities to do so. Its level of interoperability is such that it even allows its service to work with the socio-technical systems of its corporate counterparts like AWS. As a matter of fact, more than half of Ethereum's network is hosted on corporate servers, including the cloud services of AWS[3]. This situation even became a source of criticism for some who views this as creating a new form of corporate centralization.

As many other private companies that attempt to create lock-in effect when devising new products or services, AWS meanwhile attempts to restrict the interoperability of its blockchain service. It basically requires the use of its platform to use data saved on a blockchain that it manages. Even though it maintains that its blockchain infrastructure can work with the ones of other blockchains,

[3] For a breakdown of where most of Ethereum's nodes are hosted and other statistics on Ethereum's network see: https://www.ethernodes.org

including Ethereum, it actually limits their interoperability by only allowing to import data from other blockchains, but not to export it. In other words, other blockchains can work through AWS system, but no blockchains originally built using its managed blockchain service can function in another's infrastructure. At all times, AWS moreover remains in control of what can be run or not on its platform.

As a whole, the assemblage of different material and ideational elements for these six technical characteristics led to two strikingly different infrastructures. While both basically provide a service allowing their users to operate a network of actors to validate and exchange information among themselves, they do so in two very distinct ways. In line with the original beliefs of early blockchain designers, Ethereum embraces a "free market" and "infrastructural mutualism" ideologies (Swartz, 2018). By securing private ownership and creating economic incentives, it tries to push its users to actively contribute to the maintenance of its infrastructure. This represents a kind of "mutualistic self-help" where cooperation is purely driven by individual gains and guaranteed by automated contracts (Swartz, 2018, p. 10). There is in effect no social security or group protection. If mistakes or problems arise, no single actor has the legal authority to intervene as exemplified by the case of The DAO mentioned earlier (Hutten, 2019). In line with its private nature, AWS meanwhile aims to recreate clear intermediaries and controls to allow itself or the initiator of a blockchain network to police its content and users. This concomitantly contributes to further the corporate form of governance championed by the United States since the early days of the Internet. AWS and its closed network of users will in effect be responsible to implement public laws and offer an avenue for public authorities to reassert their authority over the digital economy.

Regulation and Infrastructural Contention: Between Ideas and Material Constraints

In building and maintaining their blockchain infrastructures, Ethereum and AWS do more than offer competing services. The assemblage of the socio-technical devices behind the six technical characteristics reviewed in the previous section come together to regulate the users of Ethereum and AWS' blockchains by materially embodying or, as Bruno Latour famously argued, making "durable" (1991) their respective governance ideas. Again, it represents an "architectural" form of regulation where users are constrained by their material environment rather than market, social or legal pressures (De Filippi & Wright, 2019, p. 174). If seemingly odd, this form of regulation through relatively technical decisions over who can join a specific infrastructure and how is actually quite common. As technical communities meet to devise international "best practices" or "standards" for various socio-technical systems, they are continuously regulating the environment we live in.

If durable, this paper importantly highlighted that those infrastructures are not immutable and can be re-regulated. Both Ethereum and AWS have chiefly modified the blockchain technology originally introduced in the Bitcoin whitepaper. If Ethereum remained closer to it, it still adapted it. It first and perhaps most importantly made its blockchain "Turing complete". Again, this is what allows it "to run any coin, protocol, or blockchain" (Swan, 2015, p. 21). While Bitcoin is limited to operating its sole cryptocurrency, Ethereum can be used to exchange any type of information. This technically required creating a coding script that could be translated into any programming language. Ethereum moreover created an underlying measure, *gas,* to calculate the computational efforts to execute different operations. As the smart contract that could potentially be run on its platform can deal with almost anything and significantly vary in size, this allows the price paid in Ethereum's native cryptocurrency, Ether, to the computers executing the operations on the blockchain network to vary accordingly and thereby promote competition among them.

In comparison, the changes made by AWS are obviously more substantial and run through most technical characteristics. While adopting the core idea that information can be securely exchanged via network of actors, it went to great lengths to find ways to recreate various intermediaries or what could be described as control points in its own infrastructure. To do this, it technically closed it through its credential system and removed elements of competition among members of the network by offering the computing power making the blockchain work. It also created the possibility to set private channels, which work as kinds of networks inside the broader network. As described in the previous section, all these different changes were made to recreate centralization.

Recognizing this possibility to change and contest existing infrastructures obviously begs the question of what is actually durable about them. If they can be re-regulated to fit new political-economic ideas, do they pose any real constraints or limitations? Here, it is useful to distinguish between those operating from within these infrastructures and those behind these infrastructures themselves. Private companies using the services of AWS or individuals contributing to the Ethereum network will operate according to their respective technical environment. When adding information on each blockchain or ensuring their security, the end-users of Ethereum and AWS will be constrained to follow the technical characteristics of both their infrastructures. This is not to say that some might not try to go around them. Yet, the fact that they would have to spend time and resources to do so is the very proof of the regulatory power of these technologies. In recent years, various companies have for example started to provide data analytics services aiming at uncovering the identity of Bitcoin or Ethereum users. These however require knowledge and material resources that are not readily available to most users. The existence of such “anti-

program" as Latour (1991, p. 104) would call them are thus not so much questioning the regulatory power of these infrastructures than demonstrating it.

The use of preexisting technology by both Ethereum and AWS in building their respective blockchain infrastructures meanwhile show that as new infrastructures emerge, they will themselves be shaped by the socio-technical systems they operate in. Going back to our discussion of agency in the first section of this paper, it is through their interactions with the socio-technical systems in place that Ethereum and AWS could advance their political-economic agendas. Despite both modifying the original technology of Bitcoin, their ideas that actors could form a network to exchange information was crucially shaped by it. They had to work with similar concepts, such as "nodes", "ledgers", "consensus", to adapt their technical characteristics to fit their respective political-economic ideas. Perhaps most interestingly, though, they also had to interact with other existing infrastructures to operate. Small-scale socio-technical systems, such as the blockchain infrastructures here under investigation, indeed always evolve in relation to broader infrastructures. Both blockchains were notably devised to work with the broader Internet infrastructure that connects all computers part of the network. In this case, AWS does this work by hosting the blockchain on its own servers and allowing its users to only run their blockchain on its online platform. Meanwhile, Ethereum users do not have to work *via* the data centre of the Ethereum foundation. As pointed out, they can simply download the Ethereum portal and then maintain their blockchain where they want to. AWS also connects its users to the traditional financial infrastructure by receiving its payment in fiat currencies. In contrast, Ethereum has its own cryptocurrency that enables its users to pay for executing the operations made on the blockchain.

The different decisions taken by Ethereum and AWS were thus all made in relation to preexisting socio-technical systems. In accordance with previous studies emphasizing that innovations continuously emerge from the bricolage of pre-existing material resources and ideas (Mackenzie & Pardo-Guerra, 2014; Rodima-Taylor & Grimes, 2019), it means that the shape of new infrastructures will continuously result from the productive interaction between the ideas of actors like Ethereum and AWS, and the preexisting infrastructures they plug into or interact with. The correlate of this as David Mackenzie and Juan Pablo Pardo-Guerra puts it is that "history matters" (2014, p. 157). Future decisions tend to be determined by the stock of existing resources at any point in time. This again does not mean that new infrastructures will linearly or deterministically follow one trajectory. AWS is indeed a prime example of how actors can significantly re-regulate existing technologies and develop new infrastructures. It is yet through the assemblage of existing socio-technical devices that it achieved it.

Conclusion

Throughout this paper, we argued that the building of infrastructures is a regulatory process. Looking at the recent development of blockchain services outside the financial realm by Ethereum and AWS, we showed how relatively micro and seemingly technical decisions can have regulative effects by affording different capacities and constraints to their respective users. Considering the six original characteristics of blockchain technologies that we identified, we explained how Ethereum and AWS notably aimed at defining how actors could join their respective infrastructures, what they would know of each other, how they could validate information added to the blockchain, and how they would be remunerated for their actions. These choices importantly

came to reflect two contrasting assemblages of socio-technical devices that produced two different models of governance.

By constantly attempting to ensure that its infrastructure remained as open and unmediated as possible, Ethereum promoted the techno-libertarian ideals of early cypherpunks who aimed to limit the influence of central authorities. Meanwhile, AWS precisely worked to re-create multiple intermediaries on its blockchain to retain control over its infrastructure, following a similar extractive business model than other large digital platforms commonly discussed in the literature (Srnicek, 2017; Zuboff, 2019). In doing so, we pointed out that it supported a corporate form of governance promoted by the United States since the early days of the Internet. The development of other blockchain could yet further challenge this form of governance in different ways. As Gruin (2020) notably shows, China is increasingly looking into the use of blockchains to advance its own neostatist agenda in face of the currently American-led digital economy.

We finally emphasized that both Ethereum and AWS were themselves constrained by the infrastructures that they were plugging into when developing their blockchain infrastructures. At one level, blockchains can be viewed as operating at the content layer of the Internet (De Filippi & Wright, 2019, p. 48). As they work through the Internet infrastructure to exchange information, they are to some degree just one of the many applications allowed by this broader infrastructure. As such, they had to work with the limitations of the Internet like the possibility to share the same information twice by creating a consensus system to validate information or creating specific credentials to control access to their services in the case of AWS. At the same time, we talked of blockchains as infrastructures as they are the result of the assemblage of multiple socio-technical devices that themselves enable other online services to emerge and fundamentally change how information can be shared online. If both the blockchains of Ethereum and AWS use some features

of the Internet infrastructures to operate, they do not do so similarly, and their respective users will thereby not have the same experience of the Internet. While Ethereum's users would notably be part of an open network that could *theoretically* be open to all Internet users, AWS managed blockchains' users could operate in an entirely closed environment.

This significantly goes back to our point that infrastructural change tends to occur through a process of layering rather than pure displacement of previous infrastructures. Recognizing this interestingly offers a more nuanced perspective of how markets, and in this case, digital markets, emerge not only, or even primarily, from top-down or macro-decisions by public or private actors but the continuous adaptation of small-scale socio-technical systems. Future research could look into how other technologies build or challenge pre-existing infrastructures to gain a better insight of how this process of 'infrastructuring' occurs at different scale and spaces in the global economy. We hope to have highlighted the value of this approach by looking at the case of blockchains in this paper.

Acknowledgements: The authors would like to thank both anonymous reviewers for their in-depth and insightful comments. They are also grateful to all participants to the GEM-STONES workshop "Economic Regulations in a Digital World" 25-26 as well as Andreas Dimmelmeier, Laura Gelhaus, Matthew Watson, and Jean-Frédéric Morin for providing comments on previous drafts. This project received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie Grant Agreement No 722826 and the Social Sciences and Humanities Research Council of Canada through a Connection Grant.

References

AWS. (2019). *Amazon Managed Blockchain – Deep Dive.* Amazon Web Services. Retrieved March 14th, 2020, from https://d1.awsstatic.com/events/reinvent/2019/REPEAT_1_Dive_deep_into_Managed_Blockchain_BLC301-R1.pdf

AWS. (2020a). *Amazon Managed Blockchain – Management Guide*. Amazon Web Services. Retrieved March 14th, 2020, from https://docs.aws.amazon.com/managed-

blockchain/latest/managementguide/managed-blockchain-mgmt.pdf#what-is-managed-blockchain

AWS. (2020b). *Amazon Managed Blockchain pricing*. Amazon Web Services. Retrieved March 14th, 2020, from https://aws.amazon.com/fr/managed-blockchain/pricing/

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D., & Walker, R. B. (2014). After Snowden: Rethinking the impact of surveillance. *International political sociology*, *8*(2), 121–144.

Benkler, Y. (2011a). Networks of power, degrees of freedom. *International Journal of Communication*, 5, 721–755.

Benkler, Y. (2011b). WikiLeaks and the protect-ip act: A new public-private threat to the Internet commons. *Daedalus*, 140(4), 154–64.

Bernards, N., & Campbell-Verduyn, M. (2019). Understand technological change in global finance through infrastructures. *Review of International Political Economy*, 26(5), 773–789.

Bernards, N., Campbell-Verduyn, M., Rodima-Taylor, D., Duberry, J., Dupont, Q., Dimmelmeier, A., Huetten, M., Mahrenbach, L., Porter, T., & Reinsberg, B. (2020). Interrogating technology-led experiments in sustainability governance. *Global Policy*, 11(4), 523–531.

Bradshaw, S. & Denardis, L. (2019). Privacy by infrastructure: The unresolved case of the domain name system. *Policy & Internet*, 11(1), 16–36.

Braun, B., Schindler, S. & Wille, T. (2019). Rethinking agency in International Relations: Performativity, performances and actor-network theory. *Journal of International Relations and Development*, 22(4), 787–807.

Braun, B. (2020). Central banking and the infrastructural power of finance: The case of ECB support for repo and securitization markets. *Socio-Economic Review*, 18(2), 395–418.

Brunton, F. (2019). *Digital cash: The unknown history of the anarchists, utopians, and technologists who created cryptocurrency*, Princeton University Press.

Buterin, V. (2013). *Ethereum White Paper*. GitHub. Retrieved March 14th, 2020, from https://github.com/ethereum/wiki/wiki/White-Paper.

Campbell-Verduyn, M. (2018). *Bitcoin and beyond: Cryptocurrencies, blockchains, and global governance*, Routledge.

Campbell-Verduyn, M., & Goguen, M. (2019). Blockchains, trust and action nets: extending the pathologies of financial globalization. *Global Networks*, 19(3), 308–328.

Carthwright, M. (2021). Business conflict and international law: The political economy of copyright in the United States. *Regulation and Governance*, 15(1), 152–167.

Connolly, W. (2013). The "new materialism" and the fragility of things. *Millennium*, 41, 399–412.

De Filippi, P. & Wright, A. (2018). *Blockchain and the law: The rule of code*. Harvard University Press.

Denardis, L. (2012). Hidden levers of Internet control. *Information, Communication and Society*, 15(5), 720–738.

Deibert, R. (2003). Black code: Censorship, surveillance, and the militarisation of cyberspace. *Millennium*, 32(3), 501–530.

Edwards, P. N., Bowker, G. C., Jackson, S. J., & Williams, R. (2009). Introduction: An agenda for infrastructure studies. *Journal of the Association for Information Systems*, 10(5), 364–374.

Ethereum. (2017). Ethereum Homestead Documentation: Release 0.1. Retrieved March 14th, 2020, from https://buildmedia.readthedocs.org/media/pdf/ethereum-homestead/latest/ethereum-homestead.pdf.

Ethereum. (2019). "Ethereum Improvement Proposals" Retrieved March 14th, 2020, from http://eips.ethereum.org.

Fransman, M. (2010). *The new ICT ecosystem: Implications for policy and regulation*. Cambridge University Press.

Friedman, D. (1973) *The machinery of freedom*. Open Court Publishing Company.

Garrod, J. Z. (2019). On the property of blockchains: comments on an emerging literature. *Economy and Society*, 48(4), 602–623.

Gerard, David. (2017). *Attack of the 50 foot blockchain: Bitcoin, blockchain, ethereum & smart contracts*. CreateSpace.

Goldsmith, J., & Wu., T. (2006). *Who controls the Internet? Illusions of a borderless world*. Oxford University Press.

Golumbia, D. (2016). *The politics of bitcoin: Software as right-wing extremism*. Minnesota University Press.

Gruin, J. (2020). The epistemic evolution of market authority: Big data, blockchain and China's neostatist challenge to neoliberalism. *Competition & Change*, Early Online View, 1-25.

Hsieh, Y. Y., Vergne, J. P., Anderson, P., Lakhani, K., & Reitzig, M. (2018). The internal and external governance of blockchain-based organizations. In Campbell-Verduyn (Ed.), *Bitcoin and Beyond: Cryptocurrencies, Blockchains, and Global Governance* (pp. 48–68). Routledge.

Hütten, M. (2019). The soft spot of hard code: Blockchain technology, network governance and pitfalls of technological utopianism. *Global Networks*, 19(3), 329–348.

Jeong, S. (2013). *The bitcoin protocol as law, and the politics of a stateless currency*. [Unpublished]. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2294124

Karasti, H., Millerand, F., Hine, C. M., & Bowker, G. C. (2016). Knowledge infrastructures: Part I. *Science and Technology Studies*, 29(1), 2–12.

Latour, B. (1991). Technology is power made durable. In J. Law (ed.), *A Sociology of Monsters: Essays on Power, Technology and Domination* (pp. 103-131). Routledge.

Leese, M. & Hoijtink, M. (2019). How (not) to talk about technology: International relations and the question of agency. In Hoijtink, M. & Leese, M. (Eds.), *Technology and Agency in International Relations* (pp. 1–23). Routledge.

Lessig, L. (1999). *Code and other laws of the cyberspace*. Basic Books.

Mackenzie, D. & Pardo-Guerra, J. P. (2014). Insurgent capitalism: Island, bricolage and the re-making of finance. *Economy and Society*, 43(2), 153-182.

May, T. (1994, December). Crypto anarchy and virtual communities. http://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-virtual-comm.html

McCarthy, D. R. (2013). Technology and "the international" or: How I learned to stop worrying and love determinism. *Millennium*, 41(3), 470–490.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Working Paper. https://bitcoin.org/bitcoin.pdf

Narayanan, A. & Clark., J. (2017). Bitcoin's academic pedigree. *Communications of the ACM* 60(12), 36–45.

Nestlé. (2019). Nestlé breaks new ground with open blockchain pilot. Retrieved January 11th, 2021, from https://www.nestle.com/media/pressreleases/allpressreleases/nestle-open-blockchain-pilot.

Porter, T. (2003). Technical collaboration and political conflict in the emerging regime for international financial regulation. *Review of International Political Economy*, 10(3): 520–551.

Rodima-Taylor, D., & Grimes, W. W. (2019). International remittance rails as infrastructures: embeddedness, innovation and financial access in developing economies. *Review of International Political Economy*, 26(5), 839–862.

Reinsberg, B. (2019). Blockchain technology and the governance of foreign aid. *Journal of Institutional Economics*, 15(3), 413-429.

Rothbard, M. (1970). *Power and market: Government and the economy*. Andrews McMeel Publishing.

Rosales, A. (2019). Radical rentierism: gold mining, cryptocurrency and commodity collateralization in Venezuela. *Review of International Political Economy*, 26(6), 1311-1332.

Schneider, N. (2019). Decentralization: An incomplete ambition. *Journal of Cultural Economy*, 12(4), 265-285.

Srnicek, N. (2017). *Platform capitalism*. John Wiley & Sons.

Star, S. L. (1999). The Ethnography of infrastructure. *American Behavioral Scientist*, 43(3), 377–391.

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

Swartz, L. (2018). What was bitcoin, what will it be? The techno-economic imaginaries of a new money technology. *Cultural Studies*,32(4), 623-50.

Tusikov, N. (2017). *Chokepoints: Global private regulation on the Internet*. University of California Press.

Winner, L. (1980). Do artifacts have politics? *Daedalus*, 109(1), 121–136.