Now the Code runs itself : On-chain and Off-chain governance of blockchain technology

Wessel Reijers, Iris Wuisman, Morshed Mannan, Primavera de Filippi, Christopher Wray, Vienna Rae-Looi, Angela Cubillos Vélez, Liav Orgad

NOW THE CODE RUNS ITSELF

On-chain and Off-chain Governance of Blockchain Technologies

Reijers W., Wuisman I., Mannan M., De Filippi P. & al.

Abstract

The invention of Bitcoin in 2008 as a new type of electronic cash has arguably been one of the most radical financial innovations in the last decade. Recently, developer communities of blockchain technologies have started to turn their attention towards the issue of governance. The features of blockchain governance raise questions as to tensions that might arise between a strictly "on-chain" governance system and possible applications of "off-chain" governance. In this paper, we approach these questions by reflecting on a long-running debate in legal philosophy regarding the construction of a positivist legal order. First, we argue that on-chain governance shows striking similarities with Kelsen's notion of a positivist legal order, characterised by Schmitt as the machine that runs itself. Second, we illustrate some of the problems that emerged from the application of on-chain governance, with particular reference to a calamity in a blockchain-based system called the DAO. Third, we reflect on Schmitt's argument that the coalescence of private interests is a vulnerability of positivist legal systems, and accordingly posit this as an inherent vulnerability of on-chain governance of existing blockchain-based systems.

Keywords:

Blockchain governance Kelsen Schmitt Sovereignty State of exception

Cite as:

Reijers, W., Wuisman, I., Mannan, M., De Filippi, P. (2018) « **Now the Code runs itself : On-chain and Off-chain governance of blockchain technology** » in TOPOI : International Review of Philosophy. Vol 37, Issue 17

Introduction

The invention of Bitcoin in 2008 as a new type of electronic cash has arguably brought about one of the most radical financial innovations in the last decade. In the past few years, not only has Bitcoin gained tremendous public attention, but its central architectural backbone—the blockchain—has also spread its wings into a multitude of new fields. Blockchain technologies create a 'trustless' proof mechanism for transactions between users, and allow for the registration of assets and the self-execution of software code (also known as 'smart contracts')[1]. In particular, the topic of blockchain governance has become central in the blockchain community, notably in the aftermath of the attack on 'The DAO'—a decentralized venture capital fund that was meant to be the world's first fully functioning decentralized autonomous organization (DuPont 2017). We will use The DAO attack as an illustrative case study of some of the key issues that arise in blockchain governance.

The governance of blockchain-based systems usually incorporates a variety of rules and procedures that may be implemented both 'on-chain' and 'off-chain'. *On-chain governance* refers to rules and decision-making processes that have been encoded directly into the underlying infrastructure of a blockchain-based system. This type of governance defines the rules of interactions between participants through the infrastructure within which these interactions take place; these interactions are solely determined by rules embedded within the underlying blockchain code—the so-called *rule of code* (De Filippi & Wright 2018). The rules and processes may be layered; meaning that one layer of rules is subject to another. For instance, some rules may allow for infrastructural changes by stipulating the procedures to change other (lower-level) rules, and potentially even the (higher-level) rules themselves. On-chain governance cannot be easily avoided or bypassed *stricto sensu*, because it operates according to a system of rules that have been encoded directly into the system that is responsible for enforcing them. *Off-chain governance* comprises all other (i.e. non-on-chain) rules and decision-making processes that might affect the operations and the future development of blockchain-based systems. Off-chain governance includes both endogenous and exogenous rules. The former category refers to the rules adopted

[1] Since there is a wide literature about the basics of blockchain technology (cf. Grinberg 2012; Tschorsch and Scheuermann 2016), we will not engage in a technical exposition of how it works. Instead, we will focus on the governance structures adopted by blockchain systems and communities and how these are susceptible to transform social and legal relations between people.

by a reference community to ensure the proper functioning and ongoing development of a blockchain-based system (including procedures to implement protocol changes). The latter category includes all rules imposed by a third-party onto the reference community, e.g. national laws and regulations, contractual agreements, technology standards, and so forth[2].

The ongoing debate about on-chain and off-chain governance turns on the practical question of whether existing rules and decision-making processes governing a blockchain-based system should be changed from the inside or the outside by the reference community, and whether the system should provide for a mechanism to change the governance structure itself. This practical question leads to the more theoretical and normative question of whether an existing set of code-based rules could and should overtake the exercise of human judgment in decision-making, and what are the ethical and political considerations this would entail (De Filippi & Hassan 2018). Addressing these questions brings about a new legal discourse. In an earlier paper on blockchain technology, Reyes argues that distributed ledger technology (DLT), such as blockchain technology, "will change legal discourse about the fundamental elements of legal systems, including substantive law, legal structures, and legal culture" (Reyes 2017, p. 1). The new legal discourse, she claims, "will stand on its own as a new field of legal academic inquiry and area of legal practice" (ibid, p. 63). While this observation seems correct, blockchain technology also brings to the fore ideas that have long been subject to jurisprudential debate.

This paper seeks to situate the blockchain discussion within the field of legal philosophy, examining how legal theory can apply in the context of blockchain governance. In particular, the paper explores Carl Schmitt's criticism of a positivist legal order, which he developed in contrast to the account of positivism espoused by Hans Kelsen, and how this criticism is related to the ongoing debates on blockchain governance. Our analysis includes three steps. First, we examine whether a critique of on-chain governance might parallel Schmitt's critique of Kelsen's legal positivism. Second, we consider to what extent The DAO attack and its aftermath constituted a state of exception that challenged the legal order of Ethereum's internal (on-chain) governance structure. Third, we reflect on Schmitt's argument that the coalescence of

[2] Because of these specificities, most blockchain-based systems rely on off-chain governance only in exceptional situations when on-chain governance fails or is unable to process a certain decision—for example, when a protocol change is required to improve a network's functionalities or fix technical issues that would otherwise place the whole network in jeopardy.

private interests is a vulnerability of positivist legal systems, and accordingly posit this as an inherent vulnerability of on-chain governance of existing blockchain-based systems.

On-Chain Governance: "Now the Code Runs Itself"

First, we ask whether a critique of on-chain governance might parallel Schmitt's critique of Kelsen's conception of a positivist legal order. This critique hinges on the question of whether a legal order can be self-sustaining or whether it depends on decision-making by a sovereign authority (Dyzenhaus 1994, p. 10). Off-chain governance and on-chain governance fundamentally differ along similar lines: off-chain governance allows for interventions into the blockchain protocol that are not prescribed by the protocol itself, by outside authorities. In other words, with off-chain governance people are in charge of the code, without their actions being determined by it. However, off-chain governance introduces the problem of personal sovereignty (e.g. strong individuals dominating decision-making processes). At first blush, therefore, on-chain governance seems to be the preferable mode of governance for blockchain-based systems because it ensures that no individual or group of individuals can impose their will on the blockchain community at large. Such a mode of governance seems to embrace a number of central premises of legal positivism, notably of the type of positivism espoused by Kelsen.

According to Kelsen, a positivist legal order enables a peaceful and legitimate resolution of disputes in a pluralist society, without recourse to external sources (moral or political) to justify its legitimacy. Kelsen believed that laws are valid if promulgated in accordance with the 'basic norm' of the legal order and with the legislative procedure that is authorized by this basic norm (Vinx 2007, pp. 23, 40). He thereby emphasised the content-independence of the law's legitimacy (Hart 1994, p. 36). As Vinx explains, Kelsen denied "a necessary relation between legitimacy and justice because he wanted to attack the idea that positive law is legitimate (…) only as long as its content conforms to some absolute standard of justice external to positive law" (Vinx 2007, p. 23).

Due to its reliance on rational, factual tests to settle disputes, Kelsen's conception of law making and enforcement aims to exclude any notion of private human judgement. This is most evident in Kelsen's conception of a pure legal rule.

Voegelin, who was a doctoral student of Kelsen, condenses Kelsen's "pure legal rule" to a conditional algorithm: "If Mh + E (or Mu + E), then Z => M" from which all codes and statutes derive (Voegelin 1927, pp. 270-271). The first part of the algorithm denotes past occurrences of behaviours, either in terms of performance (Mh) or avoidance (Mu), in conjunction with events (E) that usually occur as a result of said behaviour, and the second part denotes the direction of enforcement by an official authority (Z) against the individual engaging in said human behaviour (M). For instance, if a particular behaviour in conjunction with an event constitutes the operative fact of "theft", then the official authorities are to direct their coercive powers to this operative fact. If the operative facts such as theft are defined explicitly and precisely, the room for individual judgment is narrow. Here, Voegelin argues, the emphasis of the pure legal rule rests on enforcement, whereby behaviour and events only act as conditions for action by official authorities. Thus, it does not matter *who* makes the laws (or *who* is the sovereign) as long as the mechanical process of law making and enforcement is operating properly.

Dyzenhaus argues that according to Kelsen's legal theory "the underlying concept is that no individual should be subject to the will of any other individual or group of individuals" (Dyzenhaus 1994, p. 10). In order to make this possible, the extent to which personal judgment is involved in the making and enforcing of a legal order should be reduced to a minimum. Hence, for Kelsen, at the base of a legal system does not lay a sovereign power but a 'basic norm'. To arrive at this concept, Kelsen posits the axiom that a description of what *is* the case (e.g. facts of nature) cannot account for what *ought* to be the case (i.e. a norm). For instance, the validity of the norm that one ought not to steal cannot be explained from the description of behaviour that would constitute stealing. Accordingly, Kelsen argues, "the reason for the validity of a norm can only be the validity of another norm" (Kelsen 2005, p. 194). Kelsen refers to the norm underlying a legal system, from which all other norms are derived, as the 'basic norm'. Notably, this basic norm is not posited as a rule within the system, but as a basic presupposition that supports the system from the outside. For instance, the statement that laws should be obeyed because they are issued by the sovereign would, according to Kelsen, need to admit the fundamental notion that obeying the sovereign is the presupposed basic norm (Kelsen 2005, p. 194). Consequently, the key condition for a functional legal system is that its laws are

non-contradictory—not that a legitimate sovereign authorises and enforces them (Dyzenhaus 1994, p. 11).

We can trace the logic of on-chain governance along similar lines as those prescribed by Kelsen. A striking commonality between Kelsen's legal theory and the way in which blockchain technologies function is that the validity of transactions in a blockchain-based system is not determined by the content of these transactions, but by their conformity with the consensus protocol, which is determined by a factual and objective mathematical process of verification. For instance, valid blocks with transactions on the Bitcoin blockchain are not added based on their contents (i.e. based on what is transacted, from whom to whom), but based on the operative fact of whether they comply with an algorithmic test performed by a mining node. All participants in the system must recognise this type of validity for the system to be deemed authoritative. Therefore, it is presumed that the consensus protocol of a blockchain-based system represents a shared concept of authority amongst participants. As such, Kelsen's argument that "by presupposing the basic norm (…) one ought to behave as the constitution prescribes" (Kelsen 2005, p. 202), can be reinterpreted in relation to on-chain blockchain governance: by presupposing the basic norm, one ought to behave as the consensus protocol prescribes. This basic norm is tacitly presupposed, meaning that the blockchain-based system does not itself contain a rule that prescribes it. All other decision-making rules and processes implemented in on-chain governance are derived from this basic norm and ought not to contradict it.

Hence, we can observe a striking similarity between the notion of on-chain governance and Kelsen's notion of a positivist legal order. Under this view, not only are the rules of interaction between participants dictated by the blockchain protocol, but so are the rules defining the operation of the infrastructure within which these interactions take place. Some blockchain-based systems realise this form of positivist on-chain governance by relying on code-based structures not only for the regulation of participants' behaviour, but also for the introduction of changes to the infrastructure within which participants operate. For instance, in the Tezos blockchain, the "seed protocol specifies a procedure for stakeholders to approve amendments to the protocol, including amendments to the amendment procedure itself" (Goodman 2014, p. 1). Notwithstanding the ability of individual stakeholders to change the protocol rules, once they join the system, they agree to be bound by the

current rules of the protocol, which ultimately dictates their behaviour.[3] The first rules contained in Tezos' seed protocol are meant to be highly conservative within that particular blockchain ecosystem—displacing the authority of any personalist sovereign that might want to intervene. Hence, on-chain governance realised on a blockchain-based system such as Tezos shows strong similarities with Kelsen's positivist conception of the legal order.

However, as is the case with on-chain governance, Kelsen's legal theory has not remained unchallenged. Schmitt criticises Kelsen's conception of the legal order, which, according to him, embodies the apotheosis of the enlightenment project (Dyzenhaus 1994, p. 10). In appropriating Schmitt's criticism, we notably do not intend to accept it[4], but to position it as an important challenge to positivist legal systems. Reflecting on the type of legal positivism that Kelsen's theory represents, Schmitt states:

> "The general validity of a legal prescription has become identified with the lawfulness of nature, which applies without exception. The sovereign, who in the deistic view of the world, even if conceived as residing outside the world, had remained the engineer of the great machine, has been radically pushed aside. The machine now runs by itself" (Schmitt 2005, p. 48).

To problematize the positivist understanding of the legal order, Schmitt claims that the applicability of legal norms presupposes a situation of social normality, because legal norms cannot be applied to systems in a chaotic state. Emergencies that result from chaos—such as military coups, acts of war, natural disasters, financial crises, etc. —could change the situation into abnormality. In conventional public governance, far-reaching decisions need to be taken to deal with these emergencies.

Underlying Schmitt's central points of criticism is the contention that a positivist order—the machine that runs itself—is inherently contradictory as it seeks

[3] This also accords with the way Lessig imagined the code as law, that the limitations placed by code (as opposed to simply the limitation of code) intrinsically binds the behaviour of participants (Lessig 2006). As he argued in an early paper on constitution-making in cyberspace, "While regulation in real space is primarily regulation that relies upon the cooperation of the individuals who live under the regulation, regulation in cyberspace can be something different. The code in cyberspace - the software - can enforce its control directly." (Lessig 1996, p. 899).

[4] In line with Dyzenhaus (1994, p. 19), we explicitly distance ourselves from accepting Schmitt's critique – taking heed of Schmitt's highly problematic embrace of Nazism – but instead use it as a productive critique with which positivist attempts to construct a legal order should be concerned.

to replace the role of the sovereign (who can make decisions on fundamental issues) with an impersonal system of rules (e.g. a majoritarian parliamentary democracy) where decisions may be perennially postponed through discussion (Dyzenhaus 1994, pp. 4-5; Schmitt 2005, p. 63). Such a system is impersonal, according to Schmitt, because human decision-making would be subject to an order of rules that excludes private human judgment. However, for a legal order to make sense, Schmitt purports that a situation of social normality must exist and that the sovereign is the one who decides on what constitutes this normal situation (Schmitt 2005, p. 13). His argument rests on his conception of the sovereign as the agent who decides on the exception (Schmitt 2005, p. 5)—the very concept that Kelsen sought to dissolve into the legal order (Dyzenhaus 1994, p.10). This conception of the sovereign is most clearly visible in emergency situations in which exceptional decisions are required and any attempt at banishing personal sovereignty is therefore undermined. According to Schmitt, decision-making in such instances does not and cannot be premised on existing legal norms, but instead derives from "principally unlimited authority" (Schmitt 2005, p. 12) that manifests itself when the laws that restrict the sovereign's actions are suspended.

The legal discourse on the state of exception focuses on the conflict between the integrity of the legal order and the effectiveness of a government in a state of emergency. First, a government needs to recognize an emergency that requires a suspension of the legal order. Such an emergency might require the original existing order to be changed, thereby activating the state of exception. Second, a government faces the decision of revealing that certain bodies or individuals have untrammelled authority in contravention of the original order, for example by establishing a court of martial law to preside over civilians, the authority of which is not derived from the original order. Third, a government can decide to resolve the state of exception and stipulate the new order that will ensue from it. Many constitutions of contemporary liberal democracies define a state of exception that, to some extent, suspends the original legal order. Such a state of exception has for instance been in operation during France's "permanent" state of emergency (Perolini 2017) that was initiated after the terrorist attacks in Paris in 2015. States of emergency are not only declared following political events, but also in the case of economic crises such as the financial

crises in Detroit[5] and Puerto Rico.[6] Instead of being dealt with from within the existing legal order, these emergencies entail the delegation of broad, sovereign powers to an executive or designated body to make decisions in the state of exception.

To be sure, rules governing the creation and dissolution of the state of exception might be codified in positive law. Such laws could prescribe what agencies will gain decision-making authority, in what way power of different agencies is to be balanced, and what timespan might apply to the state of emergency. Schmitt's criticism therefore does not amount to the claim that the state of emergency necessarily leads to an undoing of the original positivist legal order. For instance, two years after the state of emergency was announced in France it was dissolved, which means that the original legal order was (partially[7]) restored. However, Schmitt's central point is that the laws in operation during the time of the state of emergency operate outside of the original legal order (Dyzenhaus 2006, p. 345). In opposition to Kelsen, Schmitt argues that conflict in the state of emergency is resolved through "some personal act of will emanating from outside the law" (Dyzenhaus 1994, p. 11) and that the decision concerning the establishment of an emergency is a personal one. Hence, personal judgement is involved in the state of emergency, which leads to the *risk* of the original positivist legal order being transformed into a new one. An important historical case in this regard is the use of article 48 on the state of exception in the constitution of the Weimar Republic by its president to dissolve parliament and effectively initiate the transition from a parliamentary democracy to a totalitarian state (Agamben 2005, p. 15).

Thus, Schmitt criticises Kelsen's legal positivism through the notion of the state of exception. As such, Schmitt's characterisation of Kelsen's vision of a legal order as a machine that runs itself can be translated into a formulation of on-chain governance: *now the code runs itself*. Given the similarities that we observed between Kelsen's theory and on-chain governance, we accordingly ask whether a criticism

[5] Public Act No. 436 (2013) in Michigan is a recent example of a legislative response to a state of emergency being declared due to financial crises in Detroit - granting an emergency manager extensive powers in achieving a financial rehabilitation plan, including the right to make binding orders on elected officials.

[6] The Puerto Rico Emergency Moratorium and Financial Rehabilitation Act (2016) is another example of such a response to impending debt default. For a historical account, Agamben (2005, pp. 10-22) traces the parallels between military and economic emergencies throughout the 20th century.

[7] President Macron's decision to replace the state of emergency with a new counterterrorist law has led some commentators to argue that in fact a permanent state of emergency has been put into effect (McQueen 2017).

similar to the one Schmitt put forward could apply to the practical operation of blockchain-based systems. In what follows, we first examine a particular event, the DAO attack, which elucidates some of the practical challenges of on-chain governance. This examination will lead us to an interpretation of the DAO attack as a state of exception in the context of on-chain governance.

The DAO Attack

Some of the landmark experiments with blockchain-based governance are the so-called "decentralised autonomous organisations" ("DAOs"). In a nutshell, a DAO is a code-based system with internal capital that lives on the blockchain and operates autonomously, yet relies on individuals to perform certain tasks that the code cannot do. As such, it can be regarded as an algorithmically governed organisation that responds both to automated code-based rules and deliberate human input (DuPont 2017, p. 159). The idea is to have automation at the centre and humans at the edges (Buterin 2014). One of the first real-world implementations of this concept was created in April 2016, after the company Slock.it developed a decentralized investment fund (called 'The DAO'), which was deployed on the Ethereum blockchain. People that invested money into the fund could directly participate into the governance thereof by selecting the projects that they would like the fund to invest in. The DAO was operated through a set of code-based rules ("smart contracts") to automatically execute payments when certain conditions are met (Norta 2015, p. 1). The DAO had its own forum ("DAOhub"), where most of the deliberations took place and a few prominent figures from the Ethereum community agreed to act as "curators" for the platform.

The DAO attracted considerable attention from its earliest stages. When it initiated its first round of crowd funding, it raised in 28 days the equivalent of US$150 million worth of ether (the cryptocurrency native to the Ethereum blockchain) from thousands of investors. As one of the largest crowdfunding campaign to date, the popularity of The DAO led the demand for ether to soar, bringing its market capitalization beyond US$1 billion (Ryan 2016). However, the backers of The DAO had broader ambitions: their goal was not only to provide a new means for decentralising crowd funding, but also to provide the underlying framework upon which future DAOs could be built (DuPont 2017, p. 158).

Unfortunately, the experiment was short-lived. Several warnings were raised of potential security risks, and the curators initiated a call for a moratorium on funding proposals (Mark et al. 2016). Yet, shortly after The DAO went live, an anonymous attacker started to drain ether out of the fund by exploiting a vulnerability in the smart contract governing The DAO, which allowed him/her to repeatedly execute withdrawal transactions (Daian 2016; Pfeffer 2016). A total of 3.6 million ether - worth approximately US$55 million at the time and amounting to about 30% of the total funds raised - were siphoned into another DAO ("The Dark DAO"), created by the hacker for the purpose of the attack. The DAO governance, as codified within the smart contract, lacked a rule on how to deal with this situation. There was a general rule permitting an upgrade of the smart contract code, but it did not provide a means to retrieve the stolen funds. The DAO attack revealed shortcomings not only in the governance of The DAO, but also in that of the Ethereum community as a whole. It exposed the limitation of on-chain governance that challenged the underlying principles of the Ethereum network, and other blockchain networks (DuPont 2017, p. 157): the factual verification of transactions (based on formal compliance with the protocol, as opposed to their content) and the immutability and irrevocability of such transactions, once they have been recorded onto the blockchain.

The DAO attack triggered fiery discussions within the Ethereum community.[8] Different follow-up steps were discussed and supported by different groups. Several community members advocated 'doing nothing' (echoing the 'code is law' adage). Some wanted to proceed with the freezing of all ether stored in The DAO and child DAOs, while others believed that the only way forward was to perform a hard fork, changing the protocol of the Ethereum blockchain in order to move all funds tied to The DAO (including those drained by the hacker) to a new smart contract that would enable the investors to withdraw their funds. The latter option violated the immutability ethos prevalent in most blockchain-based networks, favouring instead a distributed consensus approach, whereby changes in the blockchain protocol are deemed to be legitimate insofar the community consents to these changes. In the meantime, the attacker wrote an open letter stating that, under the 'code is law'

[8] See the relevant Reddit discussions here: https://www.reddit.com/r/TheDao/comments/4oisep/ether_safe_but_dao_cancelled_were_getting_a_refund/; https://www.reddit.com/r/ethereum/comments/4oiqj7/critical_update_re_dao_vulnerability/ also nicely visualized here: https://dao.consider.it/hard-fork-to-revert-stolen-dao-funds?results=true. Cited 30 July 2018.

principle, the ether had been legitimately acquired as per the terms of the smart contract - referring to the following terms of the DAO: "Nothing in this explanation of terms or in any other document or communication may modify or add any additional obligations or guarantees beyond those set forth in The DAO's code (....) The DAO's code controls and sets forth all terms of The DAO Creation."[9]

At the core of these discussions was the question of whether a hard fork was a legitimate response to The DAO attack. A hard fork is a change in the blockchain protocol that is not backward compatible with the previous protocol—thus creating a separate blockchain that people have to voluntarily switch to.[10] Hard forks occur repeatedly in the Ethereum network in order to fix bugs, improve the scalability of the network, or more generally, transition to a superior consensus protocol. Some of these hard forks are required in order to implement a technical fix, others are planned as part of the long-term roadmap of Ethereum (Gupta 2015; Wood 2015), but all are related to a technical issue that needs to be resolved. What made this hard fork exceptional was that it was unplanned, in response to a contentious political and moral issue, rather than a previously acknowledged technical issue. The implementation of this hard fork necessitated a departure from the existing on-chain governance structure of the Ethereum blockchain—one where the order is established, only and exclusively, by the underlying blockchain protocol. As the protocol did not include the possibility of freezing the funds or reversing the contentious transaction to restore the original state of affairs, any attempt at achieving these results would go against the integrity of the system.

Opponents to the hard fork warned of a slippery slope: once it is deemed acceptable to modify a protocol for political, as opposed to technical, reasons, it might compromise the much-touted immutability and reliability of the Ethereum blockchain as a record of truth. Some of the opponents also claimed that such a hard fork was ultimately a 'bailout' intended to protect the core development team, which was

[9] See https://pastebin.com/CcGUBgDG. Cited 30 July 2018. It should be noted that the authenticity of this letter is disputed, but as DuPont (2017, p. 174) notes, it nonetheless reflects the view of many in the Ethereum community at the time.

[10] Forking is a commonly accepted, though exceptional, practice in open source software development (Robles and González-Barahona 2012). Nyman and Lindman argue that it is a "central freedom" in open source licensing (Nyman and Lindman 2013, pp. 7-8). In blockchain-based systems, soft forks involve a temporary split of a blockchain as part of a software protocol upgrade, in which the original blockchain accrues blocks validated by non-upgraded and upgraded nodes (i.e. is backwards compatible) and the forked blockchain accrues blocks only from upgraded nodes which, following the implementation of the soft fork, tries to achieve a majority of hashing power so that the forked chain reflects the truest sequence of events (Acheson 2018).

heavily invested in The DAO and thus faced potential conflicts of interest. Instead, it was contended that The DAO should be allowed to 'fail' and that the Ethereum Foundation should not engage in the governance of individual projects such as The DAO. Arguments used by those in favour of taking action were mostly grounded in political considerations: humans should still have the final say based on social consensus, the exploit was significant enough to justify action, and, lastly, taking action would keep regulators out of the debate. Some conceded that 'flexible and pragmatic' governance was desirable and that full decentralization, autonomy and algorithmic authority could be realised once Ethereum had reached maturity (DuPont 2017, pp. 168-169).

These different views were gauged through opinions expressed on online forums such as Reddit, private discussions held with large exchanges and miners, as well as through the votes cast by ether and DAO token holders. Eventually, the Ethereum core development team released new software with an upgrade of the protocol: 89% of the miners voted in favour of the hard fork, whereas 11% decided to remain on the original blockchain. This resulted in the creation of two separate blockchains: 'Ethereum Classic' run in accordance with the original protocol, alongside the new 'Ethereum' blockchain, governed by an upgraded protocol. The reverberations of this event were felt for a long time, with the price of ether taking close to a year to recover.

Having outlined the course of events in the wake of the DAO attack, we argue that it is similar to the state of exception as conceptualised by Schmitt in several ways. First, a situation of social normality was disrupted by the act of a single agent who radically altered the distribution of funds within the system, thereby initiating a situation similar to, for instance, a financial crisis. This rupture from the anticipated course of events caused by The DAO attack is comparable to political emergencies in a situation of abnormality. Second, the new situation of abnormality brought about the necessity for a decision but could not be resolved by means of existing on-chain procedures or accepted off-chain processes (e.g. a soft fork). It therefore necessitated recourse to measures that were not covered by the existing legal order, by the existing rules and procedures on the blockchain protocol. Third, the state of exception had to be declared in order to be put into effect, which happened when a group of Ethereum developers in a closed communication channel developed the strategy to get the major cryptocurrency exchanges to halt trading activities (Dupont 2017, p. 163). Fourth, the

state of exception effectively resulted in a new legal order that was implemented through the hard fork.

We should also, however, observe some important differences between the DAO Attack and the state of exception as discussed by Schmitt. First, in contrast to liberal democracies the Ethereum community had not developed any positive laws or on-chain rules and procedures that would regulate a potential state of exception. No procedures existed that regulated which agents should have the authority to decide on the exception, what delegation of powers should apply, and what time schedule should be in effect. Second, the parties involved in the DAO Attack differ substantially from those involved in the managing of states of emergencies in modern states. Even though one might speak of the validating nodes in a blockchain-based system as a 'parliament of miners', the system does not provide for any public offices such as those of president or judge. Notwithstanding these differences, however, the similarities seem to warrant the claim that the state of exception is a challenge to the notion of on-chain governance, especially considering potential future developments of blockchain-based systems.

The Coalescence of Private Participants

Thus far, we have argued that (1) on-chain governance is similar to Kelsen's conception of the positive legal order and (2) the DAO attack shows that the state of exception poses a challenge to on-chain governance. However, we have not yet elucidated a more general insight for the governance of blockchain-based systems. One might argue that the DAO attack and its response, even while having been in a sense a state of exception, constituted a one-off event and did not expose any inherent vulnerability in on-chain governance. We return to Schmitt's critique of the positivist legal order in order to argue against such a view and to flag the inherent vulnerability of on-chain governance to the coalescence of private participants, which became evident in the wake of the DAO attack.

A central point of Schmitt's critique, springing from his notion of politics, concerns the vulnerability of positivist legal systems to the "growth of private

powers"[11] (Dyzenhaus 1994, p. 13). Schmitt argues that Kelsen's legal positivism equates legitimacy (i.e. the justification of a legal order) with formal legality (i.e. with validity of legal prescriptions), which does not account for the content of the rules and therefore lacks a substantive conception of the common good (Dyzenhaus 1994, p. 12).[12] Schmitt attributes this procedural conception of legitimacy to parliamentary, liberal democracy. He contends that the concrete liberal order cannot accept any substantive notion of the common good as the basis of its legitimacy, but can instead only rely on a procedural conception of how a shared understanding of the common good is to be arrived at, for instance through structured debate and voting in parliament. In other words, private actors in a liberal democracy cannot appeal to a higher notion of the common good, but only to the procedures that define their interactions in a decision-making process. Even though a blockchain-based system is far from the equivalent of a liberal parliamentary democracy, it shares this particular feature in that a conception of the common good of its reference community can solely be based on a procedural conception of legitimacy.

According to Schmitt, this feature of positivist legal systems provides a fertile ground for powerful, competing private interests to arise. The inherent contradiction in the legal positivist system, according to Schmitt, is that all private participants who are subject to a particular legal order also expect that those who decide subject themselves to the same legal order. The content of this legal order—which consists only of formal legality—is therefore empty and can only result from negotiations between private participants. Because the legal system is incapable of distinguishing between right and wrong (i.e. incapable of being grounded in a substantive notion of the common good), the capacity to do so is delegated to private participants. They can organise themselves into what Schmitt designates as civil society, which encompasses non-state actors such as civil society organisations (CSOs) and corporations. A crucial point is that private participants will have to coalesce in order to provide substance for the legal order. In liberal democracies, this happens through the use of distinctive liberties such as freedoms of enterprise, of association and of assembly that mobilise

[11] This problem is not unique to the blockchain ecosystem. The concept of a 'benevolent dictator' and an oligarchy among co-developers in open-source software development projects has been discussed since the 1990's (Raymond 1998).

[12] As Reijers et al. (2016) argue, the sum of individual "wills" in blockchain-based systems, represented by the nodes, do not allow for the conception of a *common will,* or common good, as it was put forward by the social contract theory of Rousseau.

powerful corporate lobby groups, CSOs and trade unions to promote private interests. Schmitt insists that this dynamic of coalescence of private participants and growth of private power is inherent to parliamentary liberal democracies and ultimately poses a risk of subverting the legal order, notably in a state of exception when a decision based on a substantive notion of the common good is called for.

To what extent might on-chain governance of blockchain-based systems be susceptible to the vulnerability of coalescence of private participants in a similar way as are liberal parliamentary democracies, at least according to Schmitt? Considering the aftermath of the DAO attack, it appears that Schmitt's criticism has some currency. First, participants in the Ethereum community initially shared some of the commitments of legal positivism by conflating formal legality (i.e., the valid state of a blockchain-based system) with legitimacy (i.e., the justification of the authority of the system). This prevented the emergence of any grounded conception of the common good and reserved the decisions between right and wrong exclusively to individuals or particular groups in these communities. The sovereign was thereby replaced by a burgeoning civil society (Dyzenhaus 1994, p. 10), comprising private actors such as Ethereum users, miners, mining pools, exchanges, the Ethereum foundation, and so forth. Individuals and groups in such a system compete with one another and use tactics to gain prominence and power.[13]

Reflecting on this tendency of growing private powers in the context of the theory of the firm, Wright (2017) argues that all proof of work (and proof of stake) systems—the *mechanisms* that make the machine run itself—will ultimately lead to corporate consolidation or to plutocracy. This is because public blockchains are not governed according to a 'one-person, one-vote' principle. Instead, voting rights are allocated in proportion to the number of tokens or hashing power that each individual has. A plutocracy implies government or rule by the wealthy, and consequently favours private interests over the common good. Several contemporary societies implement some form of plutocracy (the United States is arguably an example), but blockchain-based systems are distinct in that they do not offer a *mixed* form of

[13] Looking at the most prominent blockchain networks— Bitcoin and Ethereum—this pattern indeed seems to be present. Both these networks suffer from a concentration of voting, or 'mining', power, with a few participants who own large portions of the available assets. In the Ethereum community, ether holders, Ethereum developers, miners and exchanges all participate in the governance of the network in order to promote their own interests, without much clarity as to which party has decisive influence (ConsenSys 2016).

decision-making (e.g. partially democratic and partially plutocratic) and implement an exclusively plutocratic governance structure, at least as long as this structure is limited to the workings of on-chain governance.

As an initial response, one might simply accept this situation and embrace plutocracy as an inevitable status quo for these communities. However, as Schmitt argues, such a status quo can be radically altered in the case of an unforeseen state of exception, which calls for an arbitrary decision to be made and responded to. In such a case, one or more private actors might arise as the sovereign by deciding on a particular course of action, thereby overriding the interests of other private actors. In the case of the DAO attack, the development team, the Ethereum Foundation and the super-nodes that were heavily invested in the DAO had a significant influence in the discussions regarding the response to the attack. Moreover, personal sovereignty within a plutocracy negates the basic principle of blockchain-based systems, according to which no individual or group *shall* be allowed to impose their will on the community. As such, we can equate Schmitt's claim that a positivist legal system bears the risk that the liberal principles that support it are contradicted, with the notion that an on-chain governance system faces, in turn, the risk that its supporting principles are contradicted.

We claim that such a contradiction is precisely what happened in the wake of the DAO attack. Core developers and members of the Ethereum Foundation preliminarily discussed options for resolving the attack behind closed doors. Some of the most prominent voices of the Ethereum community took the lead in publicly presenting possible options, often without accounting for the interests of all stakeholders. The Ethereum Foundation set the parameters for polling community opinion[14] and the core developers issued the specifications for updating the participants' software client—all in the name of the community. While the community could vote on what the default option should be, it was the Foundation that set the block number by which votes would be tallied. If we unpack the decisions that were taken when the emergency arose, we can see how a particular group of private participants decided to: recognize the factual existence of an emergency; reveal the extent of authority they possess in contravention of the existing order [i.e.,

[14] Although community votes were tallied within 12 hours of voting being opened, they accounted for only 5% of ether holders (Santos 2018, pp. 38-44).

decentralized consensus]; resolve the state of exception within a set time frame, and prefigure the order that will exist following the termination of the state of exception.

In line with Schmitt, we argue that prior to the hard fork, it was already the case that core developers and the Ethereum Foundation acted as the sovereign of the order created on the Ethereum blockchain. It could be argued that the locus of sovereign power and the exercise of sovereign powers are divided. After all, the majority of nodes needed to actively upgrade their software client for the hard fork to take effect. However, individual participants that upgraded their client, far from exercising their sovereign will, were legitimising the decision that had been made on their behalf during the state of exception. This is an illustration, in the blockchain space, of Rossiter's claim that, while most democracies provide an elected representative body with the final authority in deciding to initiate a 'constitutional dictatorship' pursuant to an emergency, it is usually the parties that wield emergency powers who decide whether an emergency exists in the first place (Rossiter 1948, p. 299). We might clarify this point by drawing an analogy with Roman law. When the Roman Senate sensed danger to the Roman Republic, it could issue a decree declaring a *tumultus* (e.g. insurrection, foreign war) and call upon everyone, from consuls to ordinary citizens, to take measures to protect the Republic (Agamben 2005, p. 42).[15] By following through, the citizenry gave democratic backing to a sovereign decision, and thereby to the particular entity that made the decision. This political situation concentrates power more radically than plutocracy, as it reveals that a *particular* group can act beyond the legal order by exerting its will on the community.

The communities surrounding a blockchain-based system should not be conflated with traditional political communities, or citizens of a particular nation state. What currently sets blockchain-based systems apart from nation states is their much more radically voluntary character: all participants are free to leave or to implement a hard fork in order to establish a new voluntary community. The possibility of exiting the original community at little to no cost diminishes the need to voice dissatisfaction and resolve problems within the same political community (Hirschman 1972, p. 43). In the DAO attack, those rejecting the hard fork have effectively "left" the Ethereum community by selecting the Ethereum Classic blockchain as the authoritative blockchain. However, community members are free to

[15] The decree declaring tumultus was distinct from the decree proclaiming a *iustitium* - or a standstill of the law - that could follow.

participate in both blockchain-based systems (Ethereum and Ethereum Classic) should they see any value in doing so. We may thus discern two communities with potentially overlapping membership. Only the community members who decided to participate only in the original network and boycott the upgraded network might be said to have retained their original ideology.

However, two issues should be kept in mind. First, dealing with states of exception in blockchain-based systems will become an increasingly contentious and problematic matter when the stakes of the participants become higher. In the event that a hard fork would decimate the wealth of all participants who oppose a particular state of emergency, the existing strategy could hardly be conceived of as a voluntary response. Second, the state of exception will become more pressing once open blockchain architectures become increasingly used in commerce or by governments (for instance when these systems become general-purpose technologies or provide basic public goods). If and when utopian visions of cloud communities (Orgad & Bauböck 2018)—such as those expressed by the Bitnation project (Atzori 2015)—become a reality and refugee communities engage in self-governance by providing themselves with identity services or property right regimes, any violation of the on-chain governance structure could create crises and conflicts in the realm of off-chain governance (e.g., threats between participants, physical violence). Even though the second point, in particular, refers to a speculative state of affairs, the pace of technological change and its consequential impact urge us to discuss these issues. Mechanisms should be put in place to discourage excessive reliance on the exit strategy, and to implement instead more meaningfully and cost-effective ways to express the community's diverse voices.

Concluding Remarks

This article has shown that the ideal of on-chain governance has striking similarities with Kelsen's positivist notion of the legal order, which presupposes that no individual or group of individuals should be allowed to enforce their will on others and that individual sovereignty should be minimised in the decision-making process. At first blush, blockchain-based systems seem to provide the technological apparatus for realising Kelsen's vision of a content-independent understanding of law, where formal legality is equated with legitimacy and personal sovereignty is dissolved into

the legal order. However, in doing so, blockchain-based systems become vulnerable to the rise of private interests using off-chain mechanisms to usurp the system of on-chain governance. This risk becomes most apparent during states of exception, such as the DAO attack discussed above, when personal authority asserts itself. This case indicates that while the 'rule of code' may be formalistically followed within a particular on-chain order, sovereignty asserts itself through off-chain mechanisms during the state of exception. In light of these traits, extant blockchain governance regimes need to be carefully reconsidered and aligned with the ideology of their relevant communities.

Future research can consider the steps that blockchain communities may take to resolve states of exception, in a manner that is consonant with their respective ideologies. Such research could, for instance, aim to examine the role of the Ethereum foundation in both proclaiming the state of exception and acting upon it in the event of the DAO attack. A promising way to approach the difficulty of institutionalising the state of emergency for blockchain-based systems would be to consider Rossiter's (1948) model of "constitutional dictatorship", which confronts states of exceptions in a manner that preserves, rather than threatens, liberal democracy and civil rights. Other avenues of research to consider would be to reflect on Heller's notion of "ethical fundamental principles of law", as discussed in a recent article by Dyzenhaus (2015, p. 353), or the political philosophy of Strauss, which was largely a response to Schmitt's devastating criticism of liberal ideology and which called for the recovery of a classical perspective on politics (Howse 1997, p. 92).

References

Acheson N (2018) Hard Fork vs. Soft Fork. CoinDesk, 16 March 2018. https://www.coindesk.com/information/hard-fork-vs-soft-fork/. Cited on 30 July 2018

Agamben G (2005) State of Exception. The University of Chicago Press, Chicago

Bohr J, Bashir M (2014) Who Uses Bitcoin? An Exploration of the Bitcoin community. In: Miri A. et al. (eds) 2014 Twelfth Annual Conference on Privacy, Security and Trust (PST), Toronto, July 2014. IEEE, 94–101

Buterin V 2014, DAOs, DACs, DAs and More: An Incomplete Terminology Guide. Ethereum Blog, 6 May 2014. https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/. Cited on 30 July 2018.

ConsenSys (2016) The DAO Heist FAQ Part II. Medium, 6 July 2016. https://media.consensys.net/the-dao-heist-faq-part-ii-b10ce890ffdf. Cited on 30 July 2018.

Cunningham A (2016) Decentralisation, Distrust & Fear of the Body - The Worrying Rise of Crypto-Law, SCRIPTed 13(3): 235-257.

Daian P (2016) Analysis of the DAO exploit. Hacking, Distributed, 18 June 2016. http://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/. Cited on 30 July 2018.

De Filippi P, Hassan S (2016) Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code. First Monday 21(12).

De Filippi P, Loveluck B (2016) The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure. Internet Policy Review 5(3): 1-28.

De Filippi P, Wright A (2018) Blockchain and the Law: the Rule of Code. Harvard University Press.

Dupont Q (2017) Experiments in Algorithmic Governance : A history and ethnography of "The DAO," a failed Decentralized Autonomous Organization. In: Campbell-Verduyn, M (ed) Bitcoin and Beyond, Routledge, London

Dyzenhaus D (1994) Now the Machine Runs Itself. Cardozo L. Rev. 16(1): 1–19

Dyzenhaus D (2006) The Constitution of Law: Legality in a Time of Emergency. Cambridge University Press, Cambridge

Dyzenhaus D (2015) Kelsen, Heller and Schmitt: Paradigms of Sovereignty Thought. Theoretical Inquiries in Law, 16(2): 337–366

Goodman LM (2014) Tezos: A Self-Amending Crypto-Ledger Position Paper. https://www.tezos.com/static/papers/position_paper.pdf. Cited 30 July 2018.

Grinberg R (2012) Bitcoin : An Innovative Alternative Digital Currency. Hastings Sci. & Tech. L.J. 4: 159-208

Gupta V (2015) The Ethereum Launch Process. Ethereum Blog, 3 March 2015. https://blog.ethereum.org/2015/03/03/ethereum-launch-process/. Cited on 30 July 2018.

Hart HLA (1994) The Concept of Law, 2nd edn, Oxford University Press, Oxford

Hirschman AO (1972) Exit, Voice and Loyalty. Harvard University Press, Cambridge

Howse R (1997) From Legitimacy to Dictatorship-and Back Again: Leo Strauss's Critique of the Anti-Liberalism of Carl Schmitt. J. L. & Jurisprudence, 77(1): 77–103.

Kelsen H (2005) Pure Theory of Law. The Lawbook Exchange, Clark

Langdridge D (2006). Ideology and Utopia: Social Psychology and the Social Imaginary of Paul Ricoeur. Theory Psychol. 16(5): 641–659.

Lessig L (1996) Reading the Constitution in Cyberspace. Emory L.J. 45(3): 869-910.

Lessig L (2006) Code version 2.0. Basic Books, New York

Mark D, Zamfir V and Sirer EG (2016) A Call for a Temporary Moratorium on The DAO. Hacking, Distributed, 27 May 2016. http://hackingdistributed.com/2016/05/27/dao-call-for-moratorium/. Cited 30 July 2018.

Nakamoto S (2008) Bitcoin : A Peer-to-Peer Electronic Cash System (White Paper). https://bitcoin.org/bitcoin.pdf. Cited 30 July 2018.

Norta A (2015) Creation of Smart-Contracting Collaborations for Decentralized Autonomous Organizations. In: Matulevičius R., Dumas M. (eds) Perspectives in Business Informatics

Research. BIR 2015. Lecture Notes in Business Information Processing, vol 229. Springer, Cham

Nyman L, Lindman J (2013) Code Forking, Governance, and Sustainability in Open Source Software. TIM Review 3(1): 7-12.

Orgad L and Bauböck R (2018) Cloud Communities : The Dawn of Global Citizenship? EUI Working Paper RSCAS 2018/28.

Perolini M (2017) France's permanent state of emergency. https://www.amnesty.org/en/latest/news/2017/09/a-permanent-state-of-emergency-in-france/. Cited on 30 July 2018.

Pfeffer J (2016) The rise of the Dark DAO. Medium, 17 June 2016. https://medium.com/@oaeee/the-rise-of-the-dark-dao-72b21a2212e3. Cited 30 July 2018.

Raymond ES (1998) Homesteading the Noosphere. http://fringe.davesource.com/Fringe/Computers/Philosophy/Homesteading_The_Noosphere/homesteading.html. Cited on 30 July 2018.

Reijers W, Brolcháin FO, Haynes P (2016) Governance in Blockchain Technologies & Social Contract Theories. Ledger Journal, 1(1): 134–151

Reyes C (2017) Conceptualizing Cryptolaw. Neb. L. Rev, 96(2): 384-445.

Robles G, González-Barahona J (2012) A Comprehensive Study of Software Forks: Dates, Reasons and Outcomes. In: Hammouda I., Lundell B., Mikkonen T., Scacchi W. (eds) Open Source Systems: Long-Term Sustainability. OSS 2012. IFIP Advances in Information and Communication Technology, vol 378. Springer, Berlin, Heidelberg

Roio D J (2013) Bitcoin, the end of the Taboo on Money. Dyne.org Digital Press, April 2013: 1–17

Rossiter C (1948) Constitutional Dictatorship: Crisis Government in the Modern Democracies. Princeton University Press, Princeton

Ryan DM (2016) The DAO: an experiment in responsibility. ESR, 23 May 2016. http://enterstageright.com/archive/articles/0516/dao.htm. Cited on 30 July 2018.

Santos F (2018) The DAO: A Million Dollar Lesson in Blockchain Governance. MA Dissertation, Talinn University of Technology, Talinn

Schmitt C (2007) Concept of the Political. University of Chicago Press, Chicago

Schmitt C (2005 [1922]) Political Theology: Four Chapters on the Concept of Sovereignty. MIT Press, Cambridge

Tschorsch F & Scheuermann B (2016) Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. IEEE Communications Surveys and Tutorials, 18(3): 2084–2123.

Tual S (2016) No DAO funds at risk following the Ethereum smart contract 'recursive call' bug discovery. Slock.it Blog, 12 June 2016. https://blog.slock.it/no-dao-funds-at-risk-following-the-ethereum-smart-contract-recursive-call-bug-discovery-29f482d348b. Cited 30 July 2018.

Voegelin E (1927) Kelsen's Pure Theory of Law. Political Sci. Q, 42(2): 268-276.

Vinx L (2007) Hans Kelsen's Pure Theory of Law: Legality and Legitimacy. Oxford University Press, Oxford

Wood G (2015) Gav's Ethereum ÐΞV Update V. Ethereum Blog, 2 March 2015. https://blog.ethereum.org/2015/03/02/gavs-ethereum-d%CE%BEv-update-v/. Cited on 30 July 2018.

Wright C (2017) Proof of Work as it Relates to the Theory of the Firm (No. A00137). Doi: https://dx.doi.org/10.2139/ssrn.2993312