Why do Public Blockchains Need Formal and Effective Internal Governance Mechanisms?

Karen YEUNG* and David GALINDO**

With the birth and rise of cryptocurrencies following the success of Bitcoin and the popularity of "Initial Coin Offerings", public awareness of blockchain technologies has substantially increased in recent years. Many blockchain advocates claim that these software artefacts enable radically new forms of decentralised governance by relying upon computational trust created via cryptographic proof, obviating the need for reliance on conventional trusted third-party intermediaries. But these claims rest on some key assumptions, which this paper subjects to critical examination. It asks: can existing mechanisms and procedures for collective decision-making of public blockchains (which we refer to as internal blockchain governance) live up to these ambitions? By drawing upon HLA Hart's Concept of Law, together with literature from regulatory governance studies, we argue that unless public blockchain systems establish formal and effective internal governance, they are unlikely to be taken up at scale as a tool for social coordination, and are thus likely to remain, at best, a marginal technology.

I. Introduction

The latest rapid decline in the value of cryptocurrencies following record highs, together with the so-called "Bitcoin Cash Wars" between two alternative versions based on competing visions and technical architectures[1] of the cryptocurrency Bitcoin Cash (itself an offspring of the original Bitcoin), has provoked lively discussion in both the

* Interdisciplinary Professorial Fellow in Law, Ethics and Informatics, Law School and School of Computer Science, the University of Birmingham, UK, and Distinguished Visiting Fellow at Melbourne Law School, Melbourne, Australia. Karen Yeung's research on blockchain governance is partly funded by a Wellcome Trust Seed Award in Humanities and Social Science, "Regulating healthcare through blockchain: Mapping the legal, ethical, technical and governance challenges", 210337/Z/18/Z. This article is based on a keynote speech delivered at the "Blockchain and Public Policy" conference, University of Groningen, 29–30 November 2018.

** Senior Lecturer in Computer Security, School of Computer Science, University of Birmingham and Head of Cryptography, Fetch.AI, Cambridge, UK, email: d.galindo@cs.bham.ac.uk

[1] Bitcoin Cash vs Bitcoin SV: Bitcoin Cash originated as a hard fork of the original Bitcoin blockchain with the main goal of increasing Bitcoin's ledger block size to achieve higher transaction processing rates. Bitcoin SV, or Bitcoin "Satoshi Vision", is the latest Bitcoin hard fork that increases the block size of Bitcoin Cash from 32 MB to a maximum of 128 MB, again to achieve extra transactions rates. At the time of writing, the market cap of Bitcoin SV is about one fourth of that of Bitcoin Cash (source coinmarketcap.com). See eg J Magas, "Opposing Bitcoin ABC and Bitcoin SV Factions' Debates Grow Heated as the Bitcoin Cash Hard Fork Draws Closer" Cointelegraph (2019), available at ⟨cointelegraph.com/news/opposing-bitcoin-abc-and-bitcoin-sv-factions-debates-grow-heated-as-the-bitcoin-cash-hard-fork-draws-closer⟩ (last accessed 4 July 2019).

European Journal of Risk Regulation, 10 (2019), pp. 359–375
doi:10.1017/err.2019.42
© Cambridge University Press

https://doi.org/10.1017/err.2019.42 Published online by Cambridge University Press

policy and technical communities about the regulation and governance of public blockchains.[2] Yet when commentators speak of "blockchain governance" or "blockchain regulation", they may be referring to one or more of the following: (a) blockchain as a technology for social coordination[3] (regulation *by* blockchain); (b) the internal governance of the blockchain community itself that comprises the decision-making apparatus that determines how the blockchain system operates (internal governance *of* blockchain); or (c) the legal regulation of blockchain systems (external regulation *over* blockchain by conventional law).[4] Yet these three different phenomena are not always clearly distinguished, and sometimes conflated, resulting in both terminological and substantive confusion.

This confusion is perhaps partly due to ambiguity associated with the meaning of the term "governance", a ubiquitous term appearing in many and varied contexts, yet often referring to different phenomena, and which may be rooted in different understandings.[5] There is a rich and extensive multi-disciplinary literature, beginning from the early 1980s,[6] that spans both law and the social sciences concerned with the phenomenon of both "governance" and "regulation", yet these are not terms of art, and their meaning is often contested.[7] Although both these terms are used in discussions about blockchain, the concept of governance, for the purposes of this paper, refers to a community's mechanisms and procedures for collective decision-making that enable ordered self-rule and is therefore a prerequisite for peaceful social cooperation.[8] In other words, for the purposes of our analysis, governance refers to the structures, institutions and procedures for collective decision-making, and is *not* to be equated with *any* form of social influence, although this latter understanding is adopted in some academic writing concerned with blockchain governance.[9] Regulation, on the other hand, is understood as a sub-set of governance (and hence sometimes referred to as "regulatory governance"). Regulation refers to *intentional* attempts within a community to manage risk or influence behaviour in order to achieve a pre-specified outcome.[10]

---

[2] See for example Rocco, "On Governance: Coordination, Layers, and Structural Integrity" *Medium* (2019), available at ⟨medium.com/alpineintel/on-governance-coordination-layers-and-structural-integrity-81a722ba1bc0⟩ and Haon, "Blockchain forks and chain splits: why we should avoid them" Good Audience (2019), available at ⟨blog.goodaudience.com/blockchain-forks-and-chain-splits-why-we-should-avoid-them-f54c693a90f1⟩ (last accessed 4 July 2019).

[3] K Yeung, "Regulation by Blockchain: the Emerging Battle for Supremacy between the Code of Law and Code as Law" (2019) 82(2) *Modern Law Review* 207–239.

[4] M Finck, *Blockchain Regulation and Governance in Europe* (Cambridge University Press 2018).

[5] M Bevir "Governance as Theory, Practice and Dilemma" in M Bevir (ed), *The SAGE Handbook of Governance* (2019).

[6] D Lēwî-Faur, "From 'Big Government' to 'Big Governance'?" in D Lēwî-Faur (ed) *Oxford Handbook of Governance* (Oxford, Oxford University Press 2012) pp 1–18.

[7] For example K Kersbergen and F Waarden, "'Governance' as a bridge between disciplines: Cross-disciplinary inspiration regarding shifts in governance and problems of governability, accountability and legitimacy (2004) 43(2) *European Journal of Political Research* 143, identify nine different ways of studying governance in social scientific literature, describing the study of governance as a "growth industry".

[8] This understanding of governance springs from Bevir's observation that "At the most general level, governance refers to theories and issues of social coordination and the nature of all patterns of rule": Bevir, supra, note 5.

[9] See eg P De Filippi and G McMullen, *Governance of blockchain systems: Governance of and by Distributed Infrastructure* (2018), available at ⟨hal.archives-ouvertes.fr/hal-02046787/⟩ (last accessed 16 July 2019).

[10] This conception of regulation reflects our common practice of referring to the regulation of particular sectors or domains, such as environmental regulation, financial regulation, workplace safety regulation and so forth.

https://doi.org/10.1017/err.2019.42 Published online by Cambridge University Press

Thus, while regulation refers to intentional action aimed at achieving a specified goal,[11] mechanisms for collective decision-making are needed to enable the social co-operation necessary for a community to govern itself in a peaceful and orderly manner, and need not be oriented towards the achievement of any particular purpose, other than the general purpose of facilitating ordered rule.

This article seeks to critically investigate the *internal governance* of public (also called "unpermissioned" or "permission-less") blockchain systems. Within the technical-developer community, a lively debate has emerged in the blogosphere concerning the desirability of "on-chain governance" – that is, encoding internal governance mechanisms into the blockchain protocol, primarily in the design and operation of various approaches to initiating and "voting" on specific proposals which are then automatically implemented once the nominated threshold for approval has been reached.[12] While recognition by the developer community of the importance of attending carefully to the internal governance of public blockchains is welcome and overdue, these debates have hitherto adopted a narrow and rather limited perspective, relying almost exclusively on economically grounded and mathematically informed game-theoretic approaches[13] in which governance is, essentially, understood as a "game". In so doing, they fail to grasp the complex and contested nature, character and challenges of governance generally, based on a naïve assumption that internal governance is simply a matter of coming up with the right voting design, which would then "solve the problem" of blockchain internal governance.[14] These discussions display little (if any) awareness of the rich and extensive body of work from politics, constitutional law or the social sciences more generally, that is concerned with critically understanding the nature and challenges of governance in human communities (including but not limited to nation states) and the importance of attending to the larger socio-cultural dynamics associated with achieving peaceful and constructive community cooperation.

The core argument of this paper is that not only is it – in practice – impossible for public blockchains to govern successfully via exclusive reliance on their technical code, but also that, without legitimate and effective internal governance of public blockchain systems that rely on *formalised and effective social mechanisms*, they are unlikely to be taken up at scale as a tool for social co-ordination (ie governance by blockchain), and are thus likely to remain, at best, a marginal technology. Instead, we are more likely to see the widespread emergence of private (ie "permissioned") blockchain systems, which necessarily require transparent and accountable internal governance mechanisms due

[11] See J Black, "Decentring Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World" (2001) 54(1) *Current Legal Problems* 103–146 and J Black, "Learning from regulatory disasters" (2014) LSE Legal Studies Working Paper No 24/2014.

[12] Representative examples are P Lucsok, "Why on-chain governance?" (27 September 2018), available at ⟨medium.com/polkadot-network/why-on-chain-governance-82ecf28f314 c⟩, GitHub, "Governance" (2019), available at ⟨github.com/paritytech/polkadot/wiki/Governance⟩ and Tezos Foundation, "A Digital Commonwealth - Tezos Foundation" available at ⟨tezos.foundation/a-digital-commonwealth⟩ (last accessed 16 July 2019).

[13] A particularly ambitious proposal is that of "Liberal Radicalism", that seeks to organise some societal functions purely by algorithms and game-theory: see V Buterin, Z Hitzig and E Glen Weyl, "Liberal Radicalism: A Flexible Design For Philanthropic Matching Funds" (2018), available at ⟨papers.ssrn.com/sol3/papers.cfm?abstract_id=3243656⟩.

[14] Finck, supra, note 4, ch 7.

https://doi.org/10.1017/err.2019.42 Published online by Cambridge University Press

to the formal authority of those with the capacity to authorise the participation of others, and to alter the design and operation of the network. By undertaking an examination of *how law governs*, we can better understand the essential characteristics that any community's collective decision-making system requires in order to provide a stable, self-sustaining system of governance. We then demonstrate why a public blockchain that seeks to rely exclusively on software code to govern its internal operations lacks these characteristics. As a result, they are likely to be unstable and highly volatile, failing to provide satisfactory and enduring foundations for the governance of communities at scale (for which the successive splits of the Bitcoin community offer a compelling illustration).

II. Current public blockchain governance

In order to understand the role and importance of internal blockchain governance, it is helpful to consider first how the internal governance of public blockchains is currently structured, drawing primarily on recent academic critiques of Bitcoin's internal governance structure and operation by way of illustration.[15] To this end, it is important to recognise that there is no standard template or model for the design and implementation of the internal decision-making structures that govern the operation of public blockchains. Rather, this is a matter for the core and founding developers, who are in essence technological entrepreneurs: free to design and implement any collective decision-making structure they so wish, provided they can establish its technical feasibility. In fact the need for formal decision-making structures and mechanisms to make decisions about the current and future operation of public blockchains is not apparent from Nakamoto's original 2007 Bitcoin White Paper (or at least, on our reading of it), in which the core foundations of the Bitcoin blockchain were famously explicated and publicised. Nakamoto's vision for a state-less currency relied critically on the operation of a decentralised database stored across a distributed computing network, secured through the operation of cryptographic protocols. This vision implicitly rests on an unstated assumption and expectation that such a system would be both self-governing and self-sustaining.[16] Nakamoto appears to have envisaged that the distributed computing network would be governed by, and operated *exclusively* through technical code, without the need to rely on conventional trusted third-party intermediaries (ie social institutions, comprised of humans and thus inescapably flawed, unpredictable and vulnerable to corruption).

It is on this basis that blockchain advocates often argue that public blockchains could radically "democratise" social organisation by rendering redundant the need for conventional third-party social intermediaries (ie states, banks/financial intermediaries). This view assumes that the blockchain software code and protocols can be relied upon exclusively to regulate the system's internal operation and functioning, so that

[15] However, much of what we describe in the following paragraphs about Bitcoin and forks can be also applied to the Ethereum permission-less blockchain.

[16] S Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", available at ⟨bitcoin.org/en/bitcoin-paper⟩ (last accessed 16 July 2019).

https://doi.org/10.1017/err.2019.42 Published online by Cambridge University Press

blockchains can, in turn, be harnessed *externally* in order to co-ordinate interaction between strangers without the need for conventional third-party intermediaries. Yet on closer inspection, this view rests on *two* related yet distinct assumptions, notably, the redundancy of:

(a) conventional third-party intermediaries (in the form of banks and national governments) to achieve peaceful social cooperation among strangers; and
(b) social (ie human) institutions, achieved through replacement of governance by code.

But while (a) may hold true, at least in terms of the internal operation of these systems, it is now clear that (b) does not, thereby undermining the validity of assertions that public blockchain could, in practice, radically democratise social organisations. In particular, Vidan and Lehdonvirta[17] have demonstrated that in practice, the operation and maintenance of the Bitcoin blockchain does *not* rely exclusively on code, but instead relies on "hybrid" forms of control, including *technical mechanisms* in the form of software code but also via economic competition (via the economic costs and incentives for mining), *informal hierarchy* (via the core developers who have privileged access rights to amend the core protocol) and *user participation* (by nodes in deciding whether or not to adopt and implement software updates). Others have vividly demonstrated that the internal governance of Bitcoin is both riddled with politics and relies on social structures and human decision-making and influence (and their inevitable human frailty) in order to maintain and sustain Bitcoin's operations.[18]

Taken together, these studies identify several features that characterise Bitcoin's current internal governance structure and practice. Firstly, Bitcoin relies on the leadership and decisions of a small, elite group of core developers who function, in effect, as an informal "executive". In open source software projects (including public blockchain projects), there is typically a group of "core developers" who are more powerful and influential than rank-and-file developers. For example, after Nakamoto handed the role of caretaker of Bitcoin to Gavin Anderson in 2011, there have been a handful of core developers who have the passwords to make changes to the core software protocol (ie. with "commit" access) even though any developer can propose changes, while Ethereum's founder, Vitalik Buterin, undertakes the role of informal chief executive for the Ethereum network.[19] Thus the governance of the two largest public blockchains, Bitcoin and Ethereum, involve a high degree of *informal* centralised power in the hand of technical experts, who are not subject to any *formal*

[17] G Vidan and V Lehdonvirta, "Mine the gap: Bitcoin and the maintenance of trustlessness" (2018) 21(1) New Media & Society 42.

[18] A Walch, "Open-Source Operational Risk: Should Public Blockchains Serve as Financial Market Infrastructures?" in D Lee Kuo Chuen and R Deng (eds), *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2* (London, Academic Press 2017) pp 243–269; N Dodd, "The Social Life of Bitcoin" (2017) 35(3) *Theory, Culture & Society* 356; P Paech, "The Governance of Blockchain Financial Networks" (2017) 80(6) *Modern Law Review* 1073.

[19] Buterin, who has been described as a "benevolent dictator" over the Ethereum network: T Friebe, "Ethereum: Governed by a benevolent dictator?" (31 October 2017) *Medium*, available at ⟨medium.com/blockchainspace/ethereum-governed-by-a-benevolent-dictator-2a2be8aa331a⟩ (last accessed 16 July 2019).

https://doi.org/10.1017/err.2019.42 Published online by Cambridge University Press

accountability mechanisms nor do they have formal responsibility for overseeing the maintenance and operation and revision of the network protocols or architecture.[20]

Secondly, the effective operation of the Bitcoin network is significantly influenced by the actions and decisions of individual "miners" (the community of nodes within the network) who direct and operate the mining pools through which multiple miners pool their computational power to undertake the mining process required to append transactions to the Bitcoin blockchain. Although Nakamoto's vision for Bitcoin was a libertarian one, based on an assumption that the task of mining would be democratised and open to all those wishing to transact on the Bitcoin network,[21] in practice, mining has become increasingly industrialised in the form of "mining pools".[22] As Vigna and Casey[23] observe,

> "ever faster, energy-hungry ASIC machines would come onto the market, spurring a relentless arms race among miners chasing the finite supply of newly issued bitcoins. The only way to win that race and stay profitable was by creating giant, data-centre based mining farms. Bitcoin mining doesn't just need hard core processing power, it also needs cheap electricity. So as is often the case, a movement with ambitions to return power to individuals, accelerated out of the garage of early enthusiasts, is becoming monopolised by centralised power . . . in which China has become the dominant player, where cheap electricity and cheap labour are available".

Thus, although the formal design of the Bitcoin network appears to rest on a distributed network of individual computing nodes contributing their processing power, in practice, once the underlying political and economic reality of Bitcoin mining is taken into account, its operation can be understood as both "socially nuanced and politically loaded".[24]

Thirdly, the stability and continued operation of the network as a single, unified albeit decentralised system, is dependent upon the willingness of miners to continue to operate and upgrade to the same software code. This dependency is a matter of considerable importance, given that it is a widely accepted tenet of software engineering that software is inevitably prone to "bugs" and is never perfect nor finished. Despite programmers' best efforts, any software that is intended to be used on an ongoing basis must be maintained, that is, developers must remain on hand to release a patch or a new version each time a critical bug is discovered.[25] Furthermore, because software interacts with other software and hardware, ongoing software maintenance is

[20] Walch, supra, note 18.

[21] Vidan and Lehdonvirta, supra, note 17, p 10.

[22] R Botsman, *Who Can You Trust?* (New York, Hachette Book Group 2017) p 214.

[23] P Vigna and M Casey, *The Age of Cryptocurrency: How Bitcoin and Digital Money are Challenging the Global Economic Order* (London, Vintage 2016).

[24] Dodd, supra, note 18, p 46.

[25] A prominent example affecting the Ethereum network took place recently, in which a scheduled update called Constantinople had to be reversed halfway through its implementation by the network when bugs therein were discovered by a team of academic researchers. The process followed is consistent with the informal governance mechanisms hereby described. See Aniket, "Ethereum Constantinople Upgrade: Things you should know",

https://doi.org/10.1017/err.2019.42 Published online by Cambridge University Press

essential, to ensure the proper functioning of interactions if one component is altered.[26] Yet because individual nodes are not obliged, either by technological compulsion or legal obligation, to upgrade their software protocols, owing to the fundamentally decentralised design of the public blockchain network, resort to social influence and persuasion is needed to ensure the stability and continued functioning of the network as a unified system. For example, following an inadvertent forking of the Bitcoin blockchain in March 2013, Bitcoin's core developers sought to persuade the biggest mining pools to forgo the Bitcoin they had earned from mining via the upgraded software, and switch to the old chain (which those miners agreed to do) in order to reverse the fork and ensure that only a single blockchain continued in operation.[27] Similarly, following the infamous DAO hack, a handful of miners refused, for ideological reasons, to upgrade their software along the lines proposed and advocated by Ethereum's core developers in order to reverse the effects of the hack, resulting in the continuation of the original blockchain (known as "Ethereum Classic").[28] Both these incidents demonstrate the extent to which reliance *on human decision-making and influence* is involved in Bitcoin governance and operation, as well as the absence of any formal internal mechanism for resolving conflict concerning the network's operation.[29] In the absence of any authoritative mechanism for determining disputes, other than through the fragmentation of the network in the form of a fork, public blockchains are perpetually vulnerable to the risk of forking, and therefore prone to the threat of instability and volatility.[30]

In other words, examination of the way in which both the Bitcoin and Ethereum blockchains have operated in practice reveals that the reality is much messier and reliant on social mechanisms in conjunction with technical mechanisms of control than the mantra (and ideology) of "code is law" that is conventionally used to describe the primary (exclusive) modality through which public blockchains are internally governed. The need to resort to *informal* internal governance mechanisms to maintain and sustain its continued operation highlights the extent to which human judgement and decision-making play an important role in Bitcoin's operation. As Dodd puts it:

> "[the] reading of Bitcoin – as a horizontal network that simply embeds trust in computer code – misses some of the reality of Bitcoin's actual operation, and

Coinmonks (2019), available at ⟨medium.com/coinmonks/ethereum-constantinople-upgrade-things-you-should-know-aa75e7655345⟩.

[26] As Vidan and Lehdonvirta observe, "any live software system is not a static artefact, but an ongoing sociotechnical project": Vidan and Lehdonvirta, supra, note 17, p 8.

[27] Walch, supra, note 18.

[28] S Falkon, "The Story of the DAO – Its History and Consequences", The Startup (2019), available at ⟨medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee⟩.

[29] Finck, supra, note 4, ch 7. Singh and Chopra make a conceptually similar claim by arguing that the inexistence of a universal mechanism to establish the correctness of smart contracts written in a Turing-complete language (such as Ethereum smart contracts) implies the need to take account of social meaning to govern blockchain systems: MP Singh and AK Chopra, "Violable Contracts and Governance for Blockchain Applications", arXiv (2018), available at ⟨arxiv.org/abs/1801.02672⟩.

[30] M Atzori, "Blockchain Technology and Decentralized Governance: is the State Still Necessary?" (2017) 6(1) *Journal of Governance and Regulation 52*.

https://doi.org/10.1017/err.2019.42 Published online by Cambridge University Press

> replicates the ideology behind it. As with all complex technical systems, social practices are crucial".[31]

Yet these social practices are not only hidden from public view, but fly in the face of Bitcoin's underlying ideology. Hence de Filippi and Lovelock[32] conclude that

> "the governance of Bitcoin relies almost exclusively on its leaders, lending credit to the view that peer production can often lead to the formation of oligarchic organisational forms. In classic Weberian terms, Bitcoin governance consists of a form of domination based on charismatic authority, largely founded on presumed technical expertise. One cannot eliminate politics by technology alone, because the governance of a technology is, itself, inherently tied to a wide range of power dynamics. So Bitcoin is mostly an invisible technology that operates mostly in the background. It is therefore all the more important to make the design choices lying behind its technical features more visible to shed light on the politics implicit in the tech design."

III. What enables large diverse communities to govern themselves in a unified, stable and self-sustaining manner?

Armed with this understanding of how public blockchains are, at present, internally governed, we now consider whether their current internal governance structures and mechanisms can be expected to provide stable, self-sustaining social co-ordination. To this end, we must first attempt to identify the necessary preconditions for any such governance system. Given that modern western European legal systems are widely readily regarded as largely operating in this manner (albeit imperfectly), our methodological approach involves reflecting on the core traits that distinguish modern legal systems from their pre-modern predecessors to order to identify and propose a set of essential characteristics that are needed to produce these governance qualities.[33] For this purpose, we return to the analytic heart of legal philosophy, by drawing directly on HLA Hart's *Concept of Law*, with the aim of extrapolating from his analysis.[34] We then consider the extent to which the design and mechanisms through which public blockchains are currently governed possess these essential features, in order to evaluate whether they can be expected to provide stable, self-sustaining social co-ordination.

[31] Dodd, supra, note 18, p 45.

[32] P De Filippi and B Loveluck, "The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure" (2016) 5(3) Internet Policy Review.

[33] See Galligan's account of the "functions" of law which he ascribes to Hart, and Galligan's scepticism about them: DJ Galligan, *Law in Modern Society* (Oxford, Oxford University Press 2006).

[34] Hart's methodological approach rooted in the tradition of analytic jurisprudence has been subject to sustained criticism from a variety of perspectives over time. In particular, to acquire a holistic understanding of modern legal systems, it is important to supplement this analytic approach with a law and society perspective; see for example, Galligan, ibid. Our present purpose in drawing on Hart's approach is narrow and limited: as an illuminating springboard for a critical interrogation of unified and self-sustaining systems of governance in order to illuminate the promise and potential of public blockchains, rather than necessarily endorsing Hart's particular theory of law in an uncritical fashion.

https://doi.org/10.1017/err.2019.42 Published online by Cambridge University Press

1. Hart's *Concept of Law*

Hart's fundamental aim in *The Concept of Law* was to identify the essential nature and character of law, to identify what is distinctive and unique about the legal systems of modern societies (as opposed to systems of ordering in pre-modern close-knit societies, for example, which operate on the basis of shared social norms and conventions). For Hart, a legal system is best understood as a unified system of primary and secondary rules: which can only be understood by distinguishing between what he refers to as the "internal" and "external" view of rules (which we elaborate on below). He posits that any modern legal system must possess three core elements:

(a) rules of recognition, that enable the primary rules of the legal system to be conclusively identified;
(b) rules of change; and
(c) an official body to authoritatively adjudicate disputes.

Each of these elements is discussed more fully below.

a. Every legal system must have "rules of recognition"

According to Hart, every legal system must have a rule for conclusive identification of the primary rules of obligation, which he calls a "rule of recognition".[35] Such a rule specifies some feature (or features), the possession of which by a suggested rule is taken as conclusive affirmative indication that it *is* a rule of the group to be supported. Rules of recognition perform the vital function of overcoming a major defect of primitive legal systems in which there is often uncertainty about the content of the relevant rules. These rules of recognition may take on a huge variety of forms, simple or complex. What is crucial is the acknowledgement of reference to the writing or inscription as *authoritative*, ie as the proper way of disposing of doubts as to the existence of the rule. Where there is such an acknowledgement, there is a very simple form of "secondary rule" – a rule for conclusive identification of the "primary rules" of obligation.[36]

b. Rules of change

According to Hart, every legal system must also clearly specify the method or process for which deliberate and authoritative changes can be made to the primary rules, thereby enabling the community to deliberately and continuously adapt to changing circumstances and needs. The existence of rules of change overcomes a further defect in primitive legal systems of not being able to make deliberate changes to the rules and thus overcomes their static quality. In the simplest form, it is a rule that empowers an individual or body of persons to introduce new primary rules for the conduct of the life of the group, or some class within it, and

[35] HLA Hart, *The Concept of Law*, 2nd edn (Oxford, Oxford University Press 1994) p 95.
[36] ibid.

https://doi.org/10.1017/err.2019.42 Published online by Cambridge University Press

to eliminate old rules.[37] These rules of change might be very simple or very complex, the powers may be unrestricted or limited, and the rules might define in more or less rigid terms the procedure to be followed in legislation.[38]

c. There must be an official agency to make authoritative determinations ("adjudication") concerning whether a primary rule has been broken.

The need for an official agency to administer sanctions for the violation of rules overcomes the problem of inefficiency, a defect of primitive legal systems in which punishments or other forms of social pressure for violation of the rules (involving physical effort or use of force) are left to individuals affected or the group at large. The minimum form of adjudication consists in such determinations, and rules which confer the power to make them (or "rules of adjudication"). Such rules will identify the individuals who are to adjudicate, and the procedure to be followed. They confer judicial powers and a special status on judicial declarations about breach of obligation. These rules again define a group of important legal concepts: in this case, the concept of judge or court, jurisdiction and judgement.[39]

In summary, Hart argued that a legal system is most illuminatingly characterised as a union of primary rules of obligation with such secondary rules of recognition, change and adjudication[40] identifying two minimum *social* conditions necessary and sufficient for the existence of a legal system that possesses these core characteristics:

> "First, rules of behaviour which are valid according to the system's ultimate criteria of validity must be generally obeyed. This condition is the only one which private citizens *need* satisfy. (They may obey 'for his part only' and from any motive whatever, though in a healthy society they will in fact often accept these rules as common standards of behaviour and acknowledge an obligation to obey them or even trace this obligation to a more general obligation to respect the constitution.) Secondly, rules of recognition specifying criteria of legal validity and its rules of change and adjudication must be effectively accepted as common public standards of official behaviour by its officials. They must regard these common standards of official behaviour and appraise critically their own and each other's deviations as lapses. (Besides these, there will be many primary

[37] ibid.

[38] Hart comments that there is clearly a very close connection between the rules of change and the rules of recognition: for where the former exists, the latter will necessarily incorporate a reference to legislation as an identifying feature of the rules, though it need not refer to all the details of procedure involved in legislation. Usually some official certificate or copy will, under the Rule of Recognition, be taken as sufficient proof of enactment: ibid, p 96.

[39] Hart comments that there are intimate connections between the rules of adjudication with the other secondary rules. A system which has rules of adjudication is necessarily also committed to a rule of recognition of an elementary and imperfect sort: this is so because if courts are empowered to make authoritative determinations of the fact that a rule has been broken, these cannot avoid being taken as authoritative determination of *what the rules are*. So the rule which confers jurisdiction will *also* be a rule of recognition, identifying the primary rules through the judgements of the courts, and these judgements will become a "source of law". Although such a simple rule of recognition will be very imperfect and be inseparable from the minimum form of jurisdiction: ibid, p 97.

[40] ibid.

https://doi.org/10.1017/err.2019.42 Published online by Cambridge University Press

rules which apply to officials in their merely personal capacity which they need only obey.)"[41]

2. Do contemporary public blockchain systems possess these essential elements?

Although public blockchains are neither intended nor designed to operate as *legal* systems, if they are to successfully fulfil the function of coordinating interaction between strangers without resort to third party intermediaries, then they must nevertheless operate as stable, self-sustaining co-ordination systems: qualities which largely characterise modern legal systems. Accordingly, the following discussion considers the extent to which the internal governance structures and mechanisms of contemporary blockchains possess the three essential characteristics identified by Hart as necessary and sufficient in modern legal systems.

a. Rules of recognition

Rules of recognition are rules that enable the primary rules of the community to be identified. The primary rules of public blockchains currently consist of its underlying open source software code and protocols through which it operates and which are, in principle, available to any user to download and run on their local computers. If, however, there are multiple versions of the software, then nodes have freedom to choose which software to run. Accordingly, public blockchains lack *secondary rules* that definitively prescribe which set of primary rules nodes are legally required, morally obliged or technically compelled to adopt. Instead, most public (permissionless) blockchains rely upon *economic incentives* (encoded into the software protocols) that are designed, based on game theoretic insights, to motivate nodes to utilise the version used to produce and validate the longest chain, otherwise they risk a rejection of their attempts at validation, and will not earn rewards for mining. Hence, the longest chain rule (which, according to the Nakamoto White Paper provides the authoritative version of the distributed record) might appear to operate as a primitive secondary rule of recognition, because it serves to identify which version of the database should prevail. However, the longest chain rule is not in fact a "rule" of either a legal, moral or technical kind (it is not technologically self-enforcing, in that the longest fork does not necessarily "kill" the shorter fork.) Rather, it is a practice that is *expected* to emerge due to the economic incentives built into the consensus mechanism which Nakamoto anticipated would give rise to a "longest chain" rule emerging as a matter of mining practice, based on the assumption that economic self-interest would motivate miners to support the longest chain. In practice, however, this has not happened because miners have multiple motivations in deciding which software to support, reflected in the recent "Bitcoin hash war" and the continuation of Ethereum Classic after a hard fork was recommended by the Ethereum core

[41] ibid, p 117. However, Hart warns that the combination of primary and secondary rules does not of itself illuminate every problem, though it is at the centre of a legal system – and as we move away from the centre, we must accommodate elements of a different character.

https://doi.org/10.1017/err.2019.42 Published online by Cambridge University Press

developers following the DAO hack. In both cases, particularly ideological commitments and views about which primary rules will best serve the future of the network resulted in some miners pursuing a mining and validation strategy that failed to conform to Nakamoto's expectations. So if there are, for example, two different versions of the software in use, resulting in the production of two distinct "forks" or "chains of transactions", miners might continue to validate both chains – with users continuing to run the software on the shorter fork, resulting in two different databases continuing to operate (that are identical up to the point at which the fork takes place). As a result, the first essential property identified by Hart is absent from the internal governance of public blockchains: they lack a "rule of recognition" that authoritatively identifies and ensures that only one set of software code prevails as the authoritative record, vividly illustrated in the event of a fork. In the event of competing primary rules (embodied in different versions of the blockchain protocol and software) it is up to individual miners to decide which version of the public blockchain software to adopt. Although there are economic incentives that would result in longest-chain rule prevailing if each and every miner operated in a commercially self-interested manner, this has not always happened, resulting in "hard forks" and hence multiple ledgers emerging – which may co-exist or could lead to one ledger prevailing over the other.

b. Rules of change

While public blockchains have very clear rules that dictate how the *ledger* itself can be altered, which are encoded in the consensus protocols and implemented via the mining process, they do not contain any *formal* procedures through which the *primary rules themselves* (ie the core software protocols) can be changed. In other words, there are no formal authoritative rules that identify the procedure through which changes can be made to the software code and enable the validation of transactions and their appending to the ledger. Instead, there is an *informal process* through which open source software is modified or changed, which relies on the charismatic authority of the "core developers" who occupy a position of informal hierarchical authority over other developers. This is perfectly illustrated by the process through which Ethereum's long-anticipated Constantinople fork was paused after a security vulnerability was found. As explained in Kim and De[42] (2019) the decision was taken during a conference call amongst the most senior Ethereum developers. Accordingly, the second property identified by Hart in any modern legal system is also absent: public blockchains lack formal procedures that specify and enable authoritative changes to the blockchain code. Rather, core developers have informal power to initiate a change to the code. But even if they issue a software update, this does not guarantee that this updated code will be implemented: because it is ultimately up to the computing nodes and miners to decide whether they wish to implement the proposed software updates. Hence the process of changing the primary rules is highly

[42] C Kim and N De, "Ethereum's Constantinople Upgrade Faces Delay Due to Security Vulnerability" *CoinDesk* (2019), available at ⟨www.coindesk.com/ethereums-constantinople-upgrade-faces-delay-due-to-security-vulnerability⟩ (last accessed 16 July 2019).

https://doi.org/10.1017/err.2019.42 Published online by Cambridge University Press

informal, unreliable and volatile. In short, there is no guaranteed way to ensure that software changes to the network protocol will be taken up across the network.

c. Authoritative determinations (adjudication) concerning violations of the primary rules

In technical terms, the primary rules of the software code cannot be "violated" because they are self-enforcing in nature. Hence there is no such thing as a technical "violation" of the rules encoded in software: they are simply executed in accordance with the terms of the code. But this does not alleviate uncertainty and disputes about whether the technical code itself accurately represents the appropriate norms that should govern the particular situation in which the encoded rule was implemented. This problem was vividly illustrated following the DAO hack, in which a hacker was able to "exploit" a vulnerability in the smart contract code built on top of the Ethereum blockchain to siphon off approximately $US 50 m to the hacker's account. The exploit was not a technical violation of the primary rules: it was merely the execution of the primary rules in accordance with the software code. Nevertheless, it clearly constituted a violation of the *intention* of the underlying principles which the DAO and their software developers intended to implement. A lively debate ensued: with the majority of participants regarding the exploit as a simple case of theft, while hardliners argued that "code is law" and that therefore the hacker should be entitled to benefit from the fruits of the hack so that an attempt to implement a hard fork would violate the core principle of immutability that lies at the heart of blockchain's value as a single and "immutable" source of truth. Yet there was no authoritative way to resolve this dispute within the network itself: although the core developers recommended and initiated a hard fork via the release of a software update which would effectively reverse the effect of the exploit, two independent chains carried on after the fork (Ethereum and Ethereum Classic) because some nodes refused to upgrade their software and continued to validate and append transactions to the original chain. Thus, the third property identified by Hart as necessary for any modern legal system is also absent: there is no official body within the blockchain network that has the power to authoritatively determine disputes concerning the application of primary rules.

IV. Prospects for public blockchains in the absence of reform to their internal governance frameworks

The preceding analysis demonstrates that the internal governance framework for public blockchains currently lack the core characteristics of modern legal systems. But should this be a matter of concern, particularly given that public blockchains are socio-technical systems built on computational code, as they are not intended to create nor operate as *legal* systems? How one responds to this question depends upon one's understanding of the promise and potential of public blockchains. If we recall that many blockchain enthusiasts claim that public blockchains could, via reliance on the security and immutability of its underlying code, democratise social coordination between

https://doi.org/10.1017/err.2019.42 Published online by Cambridge University Press

strangers,[43] then their capacity to fulfil this function depends upon the capacity of public blockchains to operate as unified, stable and self-sustaining systems of governance. Yet because the current internal governance framework upon which public blockchains currently rest lack the core characteristics which Hart identifies as essential to modern legal systems, they are prone to disunity, instability, fragmentation and ossification, discussed more fully below. Taken together, these qualities suggest that they are therefore unlikely, at least under present internal governance arrangements, to become widely taken up as a scalable tool for achieving peaceful social coordination between strangers.

1. Lack of unity

The absence of any rule of recognition (or "secondary rules") which authoritatively identifies the primary rules of public blockchain systems, fundamentally precludes these systems from operating as a unified system of governance, with the risk of forking ever-present, in which forks may be proposed by any node/user/developer. There are no formal rules and procedures that identify any minimum thresholds or procedural requirements that must be met before proposing a fork. This lack of unity might be at least partly attributable to the critical importance, within modern legal systems, of what Hart refers to as the "internal point of view" in understanding the rule of recognition. By this, Hart was referring to the perspective of a member of a group which accepts and uses the rule as a guide of conduct. To illustrate this perspective, he refers to the rules of chess: players regard the rules of chess as a common standard for all who play the game, so that if a player fails to conform (or threatens to deviate) would legitimately attract criticism and demands from others. In a similar fashion, Hart emphasises that the rule of recognition must be regarded from the internal point of view as a public, common and correct standard, and *not* as something which each official observes for his or her part only.[44] For Hart, this shared and common respect and understanding for the rule of recognition is absolutely vital: it is not merely a matter of efficiency or the health of the legal system but is logically a necessary condition of our ability to speak of the existence of a *single* legal system. By providing an authoritative mark, the rule of recognition introduces the idea of a legal *system* – for the rules are now not just a discrete unconnected set but are, in a simple way, unified. Hart observes that, even in simple cases in which the rule of recognition is simply an authoritative list of rules, we have the germ of the idea of legal validity.[45] It is the common and shared respect for the rule of recognition that provides the characteristic unity and continuity of a legal system, and this depends on acceptance of common standards of legal validity.[46]

By contrast, under public blockchain's current internal governance framework, there is no common and shared acceptance of an agreed, formal procedure through which the

[43] Atzori, supra, note 30.

[44] Hart, supra, note 35, p 116.

[45] ibid.

[46] ibid.

https://doi.org/10.1017/err.2019.42 Published online by Cambridge University Press

primary rules (comprised of the core software code and protocols upon and through which the network operates) can be recognised and authoritatively identified. Instead, public blockchains rely on economic incentives that are encoded into the blockchain protocol (eg the so-called "longest chain" rule) that, if there is a disagreement about which software version represents the rules for the blockchain, nodes can be expected, out of rational commercial self-interest, to mine the longer chain because the tokens mined on the shorter chain would not generate any mining rewards. But the experience of forking on Bitcoin (and the Ethereum hard fork following the DAO hack), demonstrates that miners do not necessarily act in predictable, rationally self-interested ways. As a result, there can be continued and ongoing uncertainty about which primary rules are authoritative, and, in turn, which copy of the ledger should be regarded as authoritative at any given point in time, seriously undermining the unity of the blockchain system.

2. Ossification

In addition, the lack of any formal rules and procedures for authoritatively changing the primary rules (ie making changes to the software code which constitute the primary rules of the network and to guarantee their implementation), undermines the capacity of the network to sustain itself over time. Hence there is ongoing risk that the code becomes "ossified" because it has no formal mechanism to enable the code to be altered in order to respond and adapt to changes in the larger environment in which the system works to meet the needs of the user community. Thus not only are there no individuals with formal responsibility for maintaining the software and addressing any "bugs" identified in the code, but if some kind of "crisis" occurs (such as the DAO hack, for example) which may require the implementation of alterations, no-one within the network has the formal responsibility to respond.[47]

3. Instability and volatility

At the same time, the ever-present risk of forking reduces both the stability and value of the entire network. As Walch[48] observes

> "if these structures fragment, there is no longer a single authoritative data structure, but many, greatly undermining the technology's service as a single, reliable source of truth".

The absence of any adjudicatory body within the network with formal responsibility to authoritatively determine disputes concerning the meaning and significance of the application of the primary rules (ie contained in the software code) means that, when disputes arise concerning whether the execution of the primary rules reflect and conform to the underlying principles of the network and how it should be expected to

[47] Walch, supra, note 18.

[48] ibid, p 15.

https://doi.org/10.1017/err.2019.42 Published online by Cambridge University Press

operate, this threatens the unity of the network, allowing rival interpretations by users (passive and active nodes), and which can precipitate the fragmentation of the network via forking.[49]

V. Conclusion

This article has critically examined the prospects of public blockchains to form the foundational governance architecture for peaceful social co-operation between strangers without the need for conventional third-party social intermediaries (ie the state, banks), based on the current internal governance frameworks upon which they operate. Their capacity to do so rests on a belief that conventional third-party or "trusted" intermediaries are no longer necessary because the blockchain code can be relied upon *exclusively* to ensure the reliability, stability and future durability of the system to facilitate the requisite trust and coordination.[50] But experience has vividly demonstrated that public blockchains are not, in practice, governed exclusively by code. Rather, their operation and continued viability inevitably and unavoidably relies on *social mechanisms* that entail reliance upon and engagement with the messy and complex realities and variety of human motivations, behaviour, and decision-making in order to ensure their continued operation and their capacity to adapt to the changing needs of their communities and their dynamic external environment.

By drawing on Hart's concept of law, which argues that modern legal system are formed by the union of a system of primary and secondary rules of recognition, change and adjudication, our analysis demonstrates that public blockchains are currently governed through primary rules (comprised of the core software protocols that constitute the network and its operation) *without* an accompanying set of "secondary rules" of recognition, change and adjudication. As a result, they cannot be expected to operate (and are unlikely to operate) as unified, self-sustaining and stable systems of governance, and this has direct implications for the promise and potential of blockchain as a mechanism for facilitating cooperation between strangers. Because public blockchains lack what Hart calls "secondary rules" of internal governance that operate in conjunction with public blockchain's primary rules (comprised of the rules encoded in the technical architecture and software through which public blockchains are configured and operationalised) they provide poor guarantees of reliability. The current reliance of public blockchains on informal social mechanisms, economic incentives and the informal charismatic authority of individual core developers to sustain their operations over time, means that these systems cannot be relied upon to provide stable, predictable and enduring

[49] The Bitcoin hash-wars offer a lesson in research methodology: the limitations of a purely theoretical approach to blockchain (ie "white paper" analysis) as opposed to one that regards its interaction with the social world and surrounding context as vital and indispensable to a clear-eyed understanding of its operation, potential and limitations. This does not, however, detract from understanding the Nakamoto White Paper as a theoretically robust and elegant proposal to the problem of cooperation between strangers – but its capacity to facilitate the delivery of essential social goods (eg facilitating social cooperation) cannot be evaluated in purely theoretical or technological terms.

[50] De Filippi and Loveluck, supra, note 32, p 11.

https://doi.org/10.1017/err.2019.42 Published online by Cambridge University Press

foundations (or what Simpson calls "predictive trust")[51] for facilitating peaceful social co-operation between strangers.

Rather, our analysis suggests that, under their current internal governance frameworks, public blockchain systems are inherently unstable and vulnerable to fragmentation in the absence of any authoritative means to identify and ensure implementation of the primary code, to authoritatively initiate and implement changes to the primary code, or any procedures for authoritatively resolving disputes arising between members of the blockchain community. Accordingly, the continued and reliable functioning of public blockchains is neither guaranteed nor predictable, given the ever-present risk of forking, undermining the unity of the system and the notion of a single chain of truth upon which the value of public blockchains as a "trustless" technology for facilitating social interaction between strangers ultimately depends. In other words, unless the internal governance of public blockchains can be reformed in ways that establish meaningful and effective "secondary rules" of recognition, change and adjudication that command the acceptance and respect of blockchain communities, they will never scale for practical use cases in the real world in ways that seriously affect the rights, interest and legitimate expectations of individuals, at least in highly industrialised countries with a deep and stable commitment to the rule of law, and will merely remain the province of hobbyists with marginal and relatively minor practical significance.

[51] TW Simpson, "Computing and the search for trust" in RH Harper (ed), *Trust, Computing and Society* (Cambridge University Press 2017) p 113.

https://doi.org/10.1017/err.2019.42 Published online by Cambridge University Press