Corporate Governance for Complex Cryptocurrencies?

A Framework for Stability and Decision Making in Blockchain-Based Organizations

this version: November 22, 2017

Author: Philipp Hacker*

Abstract:

Cryptocurrencies such as bitcoin or ethereum are gaining ground not only as alternative modes of payment, but also as platforms for financial innovation, particularly through token sales (ICOs). All of these ventures are based on decentralized, permissionless blockchain technology whose distinguishing characteristics are their openness to, and the formal equality of, participants. However, recent cryptocurrency crises have shown that these architectures lack robust governance frameworks and are therefore prone to patterns of re-centralization: they are informally dominated by coalitions of powerful players within the cryptocurrency ecosystem who may violate basic rules of the blockchain community without accountability or sanction.

Against this background, this paper makes two novel contributions. First, it suggests that cryptocurrency and token-based ecosystems can be fruitfully analyzed as *complex systems* that have been studied for decades in complexity theory and that have recently gained prominence in financial regulation, too. It applies these insights to three key case studies: the Bitcoin Hard Fork of 2013; the Ethereum hard fork of 2016, following the DAO hack; and the ongoing Bitcoin scaling debate. Second, the paper argues that complexity-induced uncertainty can be reduced, and elements of stability and order strengthened, by adapting a *corporate governance framework* to blockchain-based organizations: cryptocurrencies, and decentralized applications built on top of them via token sales. Most importantly, the resulting "comply or explain" approach combines transparency and accountability with the necessary flexibility that allows cryptocurrency developers to continue to experiment for the sake of innovation. Eventually, however, the coordination of these activities may necessitate the establishment of an "ICANN for blockchains".

keywords: blockchain; token sales; ICO; initial coin offering; governance; corporation; bitcoin; ethereum; hard fork; utility token; investment token; complexity theory; ICANN

---

* A.SK Fellow, WZB Berlin Social Science Center; Research Fellow, Centre for Law, Economics and Society, and Centre for Blockchain Technologies, both UCL; Dr. iur.; LL.M. (Yale); this paper benefitted from comments by Stefan Eich, Hermann Elendner, Florian Glatz, Steven Klein, Patrick Leyens, Hilton Root, Angela Walch and Aaron Wright, as well as audiences at the European University Institute, at the "Digital Currencies, Digital Finance and the Constitution of a New Financial Order" conference in Athens and at the workshop on "Blockchain and the Constitution of a New Financial Order" at UCL. All errors remain entirely my own.

Contents

I. Introduction

In February 2016, a group of high-level experts, including the Chief Economist of the Bank of England, recommended the use of complexity theory for the predictive modeling of behavior and outcomes on financial markets.[1] Complex systems sit between simple order and chaos; hence, they are defined, inter alia, by a tension between regularity and unpredictability. In recent years, scholarship has identified an increasing number of social systems – from the health system and traffic management to economic organizations and financial markets – that exhibit such complex patterns.

In its first part, this article seeks to apply complexity theory to a novel type of financial infrastructure: blockchain-based organizations. These fall into two main types that often, however, overlap:[2] on the one hand, they include *cryptocurrencies*, such as bitcoin or ethereum, that provide means of payment.[3] On the other hand, particularly Ethereum is also increasingly used as a basis for a broad array of *token-based ventures*, such as utility and investment tokens, built on top of Ethereum. The recent rise in token sales (also called initial coin offerings, ICOs), with more than $3 billion raised in 2017 alone through this channel, testifies to this staggering

---

[1] Stefano Battiston et al., 'Complexity theory and financial regulation. Economic policy needs interdisciplinary network analysis and behavioral modeling', 351 *Science* 818 (2016).

[2] See for a more detailed explanation Philipp Hacker and Chris Thomale, 'Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law', Working Paper (2017), 12 et seq.; Jonathan Rohr and Aaron Wright, 'Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets', Cardozo Legal Studies Research Paper No. 527 (4 October, 2017), https://ssrn.com/abstract=3048104 (accessed on October 20, 2017), 8 et seqq.

[3] Written without a capital letter, "bitcoin", "ethereum" and the names of other cryptocurrencies refer to the respective digital currency; in its capitalized version, "Bitcoin", "Ethereum" et al. denote the respective blockchain supporting the currency.

development.[4] Token-based ventures (also called decentralized applications) include, for example, decentralized storage applications (Filecoin);[5] mobile messaging platforms (Status);[6] coin convertibility applications (Bancor);[7] and building blocks for a new type of decentralized internet (Blockstack).[8] Over the last two years, regulators, policy-makers and financial service providers have become increasingly interested in blockchain-based organizations, such as cryptocurrencies[9] and token-based ventures.[10] Arguably, the inherent complexity of these systems spawns deep governance problems that call for novel responses.

---

[4] CoinSchedule, 'Cryptocurrency ICO Stats 2017', https://www.coinschedule.com/stats.php (accessed on November 6, 2017).

[5] Protocol Labs, 'Filecoin: A Decentralized Storage Network', Updated White Paper (14 August, 2017).

[6] Jarred Hope et al., 'The Status Network', White Paper (June 15, 2017).

[7] Eyal Hertzog et al., 'Bancor Protocol', White Paper (October 12, 2017).

[8] Muneeb Ali et al., 'Blockstack: A New Internet for Decentralized Applications', White Paper (October 12, 2017).

[9] See, e.g., UK Government Office for Science, 'Distributed Ledger Technology: beyond block chain (2016); European Commission, 'Consumer Financial Services Action Plan: Better Products, More Choice' COM(2017)139 final, 12-13 (announcing, inter alia, the creation of a FinTech Task Force at the Commission, and a pilot project to reinforce capacities concerning distributed ledger technology); European Parliament, 'Virtual currencies. European Parliament resolution of 26 May 2016 on virtual currencies' 2016/2007(INI) (noting high volatility, "absence of traditional forms of regulatory supervision, safeguards and protection" as well as "legal uncertainty surrounding new applications of DLT"); World Economic Forum, 'The future of financial infrastructure. An ambitious look at how blockchain can reshape financial services' (2016) (exploring nine "case deep-dives" from payment sytems via insurance to investment management and market provisioning); European Banking Association (EBA), Cryptotechnologies, a major IT innovation and catalyst for change, Report (May 11, 2015) (similarly documenting use cases in trade and finance); European Central Bank, 'Eurosystem's vision for the future of Europe's financial market infrastructure' (2016) 6 (announcing an assessment of the relevance of distributed ledger technology to European financial services and market structures); European Central Bank, 'Virtual Currency Schemes – A Further Analysis' (2015); Andrea Pinna and Wiebe Ruttenberg, 'Distributed ledger technologies in securities post-trading', European Central Bank Occasional Paper No 172/2016 (2016); European Central Bank, 'Distributed Ledger Technology' (2016) (1) In Focus; Bank of England, 'FinTech Accelerator Proof of Concept. Distributed Ledger Technology' (2016) (documenting an experimental transfer of assets using blockchain); John Barrdear and Michael Kumhof, 'The macroeconomics of central bank issued digital currencies' Bank of England Staff Working Paper No. 605 (2016); see generally http://www.bankofengland.co.uk/research/Pages/onebank/cbdc.aspx; Sead Muftic, 'Overview and Analysis of the Concept and Applications of Virtual Currencies' JRC Technical Report (2016); d'Artis Kancs et al., 'The Digital Agenda of Virtual Currencies' JRC Technical Report (2015).

[10] FCA 'Initial Coin Offerings' (12 September, 2017), https://www.fca.org.uk/news/statements/initial-coin-offerings; Australian Securities & Investments Commission, 'Initial coin offerings', Information Sheet INFO 225 (September 2017), https://www.asic.gov.au/regulatory-resources/digital-transformation/initial-coin-offerings/#what; Canadian Securities Administrators, 'Cryptocurrency Offerings', CSA Staff Notice 46-307 (24 August, 2017), http://www.osc.gov.on.ca/documents/en/SecuritiesCategory4/csa_20170824_cryptocurrency-offerings.pdf; Hong Kong Securities and Futures Commission, 'Statement on Initial Coin Offerings' (5 September, 2017), http://www.sfc.hk/edistributionWeb/gateway/EN/news-andannouncements/news/doc?refNo=17PR117; Securities Commission Malaysia, 'Initial Coin Offering', Media Statement (9 July, 2017), http://www.mondovisione.com/media-andresources/news/securities-commission-malaysia-media-statement-initial-coin-offerings/; Central Bank of the Russian Federation (Bank of Russia), 'On the Use of Private "Virtual Currencies" (Crypto Currency)', (4 September, 2017), https://www.cbr.ru/press/PR/?file=04092017_183512if2017-09-04T18_31_05.htm (all accessed on 2 November, 2017); Monetary Authority of Singapore, 'MAS Clarifies Regulatory Position on the Offer of Digital Tokens in Singapore' (1 August, 2017), http://www.mas.gov.sg/News-and-

In its second part, this paper therefore maps out regulatory implications of the complexity analysis and adapts a corporate governance framework to blockchain-based organizations. Improving the governance of these systems is crucial not only for the future of cryptocurrencies as a means of payment, but also for token sales and decentralized applications funded by them: first, these applications need a solid, predictable environment on which to run their code. Second, as the controversies surrounding Tezos tokens show,[11] token-based ventures operating on top of the Ethereum blockchain are themselves beset by significant governance problems. Arguably, token-based ventures often very much look like companies with their principals (investors) and agents (management), rather than open currency networks;[12] therefore, the corporate governance perspective befits them even more than the underlying cryptocurrency protocols like Bitcoin or Ethereum.

Cryptocurrency and token regulation in general can take two main forms. On the one hand, it may seek to mitigate exposure of the financial system at large from the volatility and systemic risk inherent in cryptocurrencies; from this perspective, regulation protects outsiders, and the financial system, from the negative externalities cryptocurrencies might impose on them.[13] This, however, presupposes a certain size of cryptocurrencies in the financial system – a size they may assume at some point, but which they probably still lack at the moment.[14] On the other hand, regulation may be required to protect cryptocurrency/token users *within* the system against information and power asymmetries, as early as the current stage of market capitalization. It is this second, internal perspective that this article adopts; however, to the extent that user protection also strengthens accountability and regularity within cryptocurrencies, it potentially has positive spillover effects for containing externalities, too.

Against this background, the article aims to make two novel contributions to the growing literature on the regulation of cryptocurrencies and token-based ventures. First, it shows that blockchain-based ecosystems exhibit the distinguishing characteristics of complex systems and can therefore be fruitfully analyzed with the tools of complexity theory. This is not a merely hypothetical proposal: complexity economics has already been successfully applied to the detection of bubbles in bitcoin prices, for example.[15] Most importantly, complex behavior is induced by imperfect governance structures that lead to unpredictable interactions between diffused agents in blockchain-based ecosystem. Despite its purportedly "trustless nature", upon closer scrutiny questions of trust between different stakeholders, and problems of the governance mechanisms that may inspire such trust, resurface prominently in blockchain environments. Second, this article shows how regulation may take inspiration from the literature

---

Publications/Media-Releases/2017/MAS-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-Singapore.aspx.

[11] See Marc Hochstein, 'Tezos Founders on ICO Controversy: 'This Will Blow Over'' (*CoinDesk*, October 25, 2017), https://www.coindesk.com/tezos-founders-ico-controversy-will-blow/.

[12] See, e.g., SEC, 'Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO', Release No. 81207 (25 July, 2017), at 12-15.

[13] See, e.g., Angela Walch, 'The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk' (2015) 18 NYU J Legislation and Public Policy 837.

[14] See, e.g., European Central Bank, 'Virtual Currency Schemes – A Further Analysis' (2015) 17.

[15] Eng-Tuck Cheah and John Fry, 'Speculative bubbles in Bitcoin markets? An empirical investigation into the fundamental value of Bitcoin' (2015) 130 *Economics Letters* 32; John Fry and Eng-Tuck Cheah, 'Negative bubbles and shocks in cryptocurrency markets' (2016) 47 *International Review of Financial Analysis* 343; David Garcia et al., 'The digital traces of bubbles: feedback cycles between socio-economic signals in the Bitcoin economy' (2014) 11 *Journal of the Royal Society Interface* 20140623; see also Adrian (Wai-Kong) Cheung, Eduardo Roca and Jen-Je Su, 'Cryptocurrency bubbles: an application of the Phillips–Shi–Yu (2013) methodology on Mt. Gox bitcoin prices' (2015) 47 *Applied Economics* 2348.

on corporate governance to remedy such governance imperfections. Particularly, it suggests the development of a Blockchain Governance Code and the compulsion of cryptocurrencies to comply with it, or to explain why they don't. The European Parliament, in its resolution on virtual currencies, warned that regulation "may not be adapted to a state of affairs which is still in flux", and therefore called for proportionate, "smart regulation" tailored to cryptocurrencies without stifling innovation;[16] the solution offered here is very much in line with these requirements. "Testing" regulation in the form of a comply or explain approach is likely to generate, over time, information and a better understanding, for regulators, of where the relevant problems lie.[17] Eventually, to coordinate these self-regulatory activities, an "ICANN for blockchains" may have to be established.[18] Arguably, a coherent and transparent governance mechanism can strengthen elements of regularity and stability within cryptocurrencies, protecting those already owning cryptocoins, making such currencies more attractive for novel users, and encouraging financial stability more broadly as cryptocurrencies and token-based ventures become more interconnected with the traditional financial system. Transparency and stability on the platform level will likely prove crucial as an increasing number of decentralized applications, such as smart contracts or token-based investment vehicles, are added onto blockchain platforms.

The remainder of the article is organized as follows. Part II provides a very brief overview of complexity theory and its applications. Part III offers a short introduction to blockchain-based systems and argues that they should be understood as complex systems. Part IV explores the regulatory consequences of this novel analysis by adapting corporate governance schemes to cryptocurrency regimes and token-based ventures. Part V concludes.

II. Chaos and Complexity Theory

Complexity, as an intermediate concept, sits between simple order on the one hand and chaos on the other. While in simply ordered systems, future development can be assessed fairly precisely (at least probabilistically),[19] chaos is defined by largely unpredictable behavior which, however, still shows some regularity or structure (and therefore can be distinguished from mere chance).[20] An example of simple order would be a snooker table on which a ball is hit. Of chaos, the development of weather systems is the best-known example;[21] the extravagant swing movements of a double pendulum are another.[22] Complexity shows elements of both of these extreme cases: of structural regularity and unpredictability.

[16] European Parliament (n 9) Art. 4, 14 and 18.

[17] Patrick Leyens, 'Comply or Explain im Europäischen Privatrecht – Erfahrungen im Europäischen Gesellschaftsrecht und Entwicklungschancen des Regelungsansatzes' (2016) ZEuP 388, 419.

[18] See below, Part IV.3. I am grateful to Aaron Wright for discussing this matter with me.

[19] Michael Strevens, Bigger Than Chaos. Understanding Complexity through Probability (Harvard University Press 2003) 5.

[20] ibid 6; Cars Hommes, *Behavioral Rationality and Heterogeneous Expectations in Complex Economic Systems* (CUP 2013) 54-58; David Levy, 'Chaos Theory and Strategy: Theory, Application, and Managerial Implications' (1994) 15 Strategic Management Journal 167, 168.

[21] William Baumol and Jess Benhabib, 'Chaos: Significance, Mechanism, and Economic Applications' (1989) 3 Journal of Economic Perspectives 77, 92; David Byrne, *Complexity Theory and the Social Sciences* (Routledge 1998) 23 and 28.

[22] Eric W Weisstein, 'Double pendulum' (2007), available at http://scienceworld.wolfram.com/physics/DoublePendulum.html.

1. Properties of Complex Systems

Complexity theory models system-environment relationships, with a focus on the interaction between system members and their spontaneous self-organization.[23] Therefore, the time dimension is of the essence. Complexity models are dynamic, describing the evolution of systems as iterative processes, where the outcome of one cycle is simultaneously the start of the next.[24]

Complex systems exhibit a variety of properties that distinguish them from ordinary, simply ordered systems. First, and most importantly, some sort of order (recurring patterns) exists, but the system over time generates outcomes that are a priori unpredictable.[25] Often, second, the system exhibits feedback effects: local interactions have global effects,[26] which in turn may influence local interactions (positive or negative feedback). Third, complex systems are marked by significant variance, i.e., actors are highly heterogeneous.[27] They may, for example, differ in their goals, motivations or degrees of rationality. Importantly, fourth, the development of the system is non-linear over time; rather, it exhibits unpredictable ruptures or changes as it drifts from one state into another.[28] For example, fluids may abruptly form honeycomb patterns (Bénard convection);[29] weather conditions may suddenly change; and financial systems become absorbed in unexpected crises.

2. Applications of Complexity Theory

Complexity theory was first introduced in the study of biological systems.[30] Since the 1990s, chaos and complexity theory have been increasingly applied to the social sciences as well.[31] Particularly, organizations were fruitfully modeled as complex institutions.[32] From there, it was but a small step to an application in economics.[33] After the stock market crash of October 19, 1987, academics began turning to non-linear models, found in non-linear dynamics and complexity theory, to explain the interaction of market participants, and of financial markets in particular.[34] Specifically, those theories are better able to model sudden changes of behavior and stark movements, such as those witnessed during financial crashes, than conventional, linear models.[35] They may thus provide some much-needed structure for such seemingly

---

[23] M Mitchell Waldrop, *Complexity. The Emerging Science at the Edge of Order and Chaos* (Simon & Schuster 1992) 11; Strevens (n 19) 7.
[24] Tim Blackman, 'Complexity theory' in Gary Browning et al. (eds), *Understanding Contemporary Society: Theories of the Present* (SAGE 2000) 139, 145.
[25] Blackman (n 24) 140.
[26] Blackman (n 24) 142.
[27] Hommes (n 20) 8-10; Strevens (n 19) 10-11.
[28] Blackman (n 24) 143.
[29] Strevens (n 19) 1.
[30] Stuart Kauffman, At Home in The Universe. The Search for Laws of Self-Organization and Complexity (OUP 1995) Chapter 1.
[31] David Harvey and Michael Read, 'The Evolution of Dissipative Social Systems' (1994) 17 Journal of Social and Evolutionary Systems 371, 373.
[32] RA Thiétart and B Forgues, 'Chaos Theory and Organization' (1995) 6 Organization Science 19.
[33] Baumol and Benhabib (n 21).
[34] David A Hsieh, 'Chaos and Nonlinear Dynamics: Application to Financial Markets' (1991) 46 Journal of Finance 1839; Edgar E. Peters, *Fractal Market Analysis. Applying Chaos Theory to Investment and Economics* (Wiley 1994).
[35] Hsieh (n 34) 1839.

random events. The contribution made by Stefan Battiston et al.[36] is, as far as can be seen, the first to apply the insights of complexity and chaos theory not only to the modeling of financial markets, but explicitly to financial regulation. The moment of its appearance is suggestive: the financial crisis has made it abundantly clear that the models used to inform financial regulation before were inadequate.[37]

III. Complex Cryptocurrencies?

This paper claims that complexity theory not only fits traditional modes of banking and finance, but also novel financial ecosystems, such as blockchain-based cryptocurrencies, and may deliver important insights into their regulation. Cryptocurrencies, such as bitcoin and ethereum, and token-based ventures running on permissionless blockchain technology are excellent candidates for complexity theory in so far as they are to a large extent self-organized. They are based on peer-to-peer systems which connect a set of nodes into a self-organizing network that anyone can join at any time;[38] and the network uses an open source software which is maintained and updated by participants.[39] In the parlance of complexity theory, there is a high degree of interconnectedness of the different independent agents.[40] As we shall see, however, centralizing elements become ever more important in times of crisis. This tension between decentralization and re-centralization, and between regularity and unpredictability, becomes apparent most prominently in the contested governance of cryptocurrencies, to which we turn (below, 2. and 3.), after a brief introduction to the technology behind blockchain.

1. The Functioning of Blockchain-Based Systems

Using a public-private key encryption protocol, a blockchain logs pieces of information, such as transactions between two users (for example: a monetary payment), on a decentralized list (the "ledger") that is stored in its entirety on many users' computers (so-called "nodes").[41] New transactions are bundled in blocks of information; they are added to the previous blocks on the ledger through a mathematical process ("mining");[42] and their authenticity is finally confirmed by the nodes via a decentralized consensus mechanism – creating a list (chain) of transaction blocks.[43] Thereby, the blockchain logs all transactions, or other changes, made to it since its inception in a database accessible from every node. Specifically, blockchain supports distributed (i.e., not centralized) ledgers.[44]

---

[36] See above (n 1).
[37] See Battiston et al. (n 1) 819.
[38] Dwyer (n 45) 81, 82; on peer-to-peer systems, see also the articles in Andy Oram (ed), *Peer-to-Peer. Harnessing the Power of Disruptive Technologies* (O'Reilly 2001).
[39] Dwyer (n 45) 82.
[40] Cf. also, for the financial system as such, Battiston et al. (n 1) 818.
[41] More precisely, these functions are only fulfilled by full nodes (as opposed to lightweight nodes), see Andreas M Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* (O'Reilly 2014) 6; the term "node" will imply "full node" in this article.
[42] Only some, not all nodes contribute to the mining process; those that do are called miners; see Antonopoulos (n 41) 1-2 and ch 8.
[43] See the "founding document" of blockchain: Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System (2008); for an introductory overview, see also Jan Witte, 'The Blockchain: A Gentle Introduction', Working Paper (2016), https://ssrn.com/abstract=2887567.
[44] Cf. UK Government Office for Science (n 9) 5; Nancy Liao, 'Symposium Introduction: Why Does Blockchain Matter?' Yale J on Regulation: Notice & Comment (June 5, 2017), http://yalejreg.com/nc/symposium-introduction-why-does-blockchain-matter/.

This distributed architecture in turn enables the most innovative feature of blockchain: a decentralized consensus mechanism that decides which chain is authentic in cases of discrepancy between different variants of the distributed ledger. Chains grow at the rate at which new blocks are added and confirmed by the community of nodes. Therefore, the longest chain, backed by the majority of users (more precisely: their computing power), is considered the consensus chain.[45] A blockchain, hence, does not rely on any "trusted third party", such as a central bank, to decide on the validity of records on the ledger.[46] Rather, being based entirely on its users and decentralized cryptographic processes, it promises a disintermediation of previously intermediated services, such as asset or money transmission (banking).[47] Furthermore, its decentralized nature makes it highly resistant to manipulation;[48] and the public-private key encryption generally implies pseudonymity.[49]

Blockchain has many potential applications, from securities transactions to smart contracts and civic participation in democracies;[50] currently, however, its innovative potential is perhaps most prominently unfolding in the rise of cryptocurrencies (also called digital or virtual currencies),[51] and decentralized applications built on top of them (such as Filecoin, Status etc.).[52] In this context, a *permissionless* variety of blockchain is most often used;[53] utility or investment tokens are generally offered on Ethereum under its ERC20 token standard.[54] The theoretical attractiveness of permissionless blockchains like Ethereum resides precisely in their openness:[55] they allow everyone to join, run a node and participate fully in the updating of the chain; however, as a nascent strand of literature shows, permissionless blockchains also exhibit

---

[45] Even more precisely, it is the chain with greatest cumulative proof-of-work difficulty, see Antonopoulos (n 41) 198-200.

[46] Nakamoto (n 43) 1.

[47] Cf. EBA (n 9); Aaron Wright and Primavera De Filippi, 'Decentralized Blockchain Technology and the Rise of Lex Cryptographia', Working Paper (2016), https://papers.ssrn.com/abstract_id=2580664, at 2.

[48] Antonopoulos (n 41) 211-213.

[49] Bonneau et al. (n 45) 116, also on the problem of re-identification.

[50] See, e.g., Wright and De Filippi (n 47) for an excellent overview.

[51] All cryptocurrencies use cryptographic techniques to function; the terminological differences between them and other digital or virtual currencies are not important for this paper (see, e.g., Lam Pak Nian and David Lee Kuo Chuen, 'Introduction to Bitcoin' in David Lee Kuo Chuen (ed) *Handbook of Digital Currency* (Elsevier 2015) 5, 6-7; Andrew Wagner, 'Digital vs. Virtual Currencies' (*Bitcoin Magazin*, August 22, 2014), https://bitcoinmagazine.com/articles/digital-vs-virtual-currencies-1408735507/; European Central Bank (n 14) 9-11); hence the term "cryptocurrencies" will be used, which denotes bitcoin, ethereum and other blockchain-based, decentralized currencies studied in this article.

[52] For an overview of these applications, see, e.g., Hacker/Thomale (n 2) 11-13; Rohr/Wright (n 2) 12-24.

[53] Permissionless (also called public) blockchains can be joined by anyone at any time, typically under conditions of pseudonymity or anonymity, and any user can add transactions and update the chain by mining (BitFury Group & Jeff Garzik, 'Public versus Private Blockchains: Part II: Permissionless Blockchains' (2015) 2); access to and functions within permissioned (also called private) blockchains, by contrast, are restricted and typically coupled to an identity management system (see, e.g., Tim Swanson, 'Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems' (2016) 5); banks, for example, experiment mainly with permissioned blockchains as novel transaction systems (ibid 6; BitFury Group & Jeff Garzik, Public versus Private Blockchains: Part I: Permissioned Blockchains (2015) 3-5; see also Christian Cachin, 'Architecture of the Hyperledger Blockchain Fabric' (2016)). This article focuses on permissionless blockchains as they are employed by cryptocurrencies.

[54] Rohr/Wright (n 2) 12 et seq.

[55] Cf. Philipp Paech, 'The Governance of Blockchain Financial Networks' Modern Law Review (forthcoming), https://ssrn.com/abstract=2875487, 14.

significant governance problems.[56] The technology was first described in a paper introducing the bitcoin cryptocurrency in late 2008.[57] Since then, a number of alternative money networks have started their own blockchain, giving rise to a range of cryptocurrencies.[58] As mentioned, they have garnered significant attention from regulators, policy-makers and financial service providers.[59] As the market capitalization of these currencies rises,[60] and as they become more integrated into the economy as an accepted means of payment,[61] the question of a suitable regulatory environment becomes ever more pressing. The same holds true for the decentralized applications built on top of them, which are raising billions of dollars with, until now, very limited regulatory oversight.[62]

2. Imperfect Governance Structures

Governance is a key concept in studies on the internet ecosystem,[63] but it can be fruitfully applied to blockchain ecosystems as well. Governance is generally understood as a system shaping coordination between different actors. In a recent paper, Jeanette Hofmann et al. propose that "[g]overnance […] should be defined as coordinating coordination or *reflexive coordination*, because it questions and potentially redefines the rules of the game."[64] In turn, coordination "becomes reflexive when ordinary interactions break down or become problematic […] and we see ourselves forced to discuss and negotiate the underlying norms, expectations and assumptions that guide our actions".[65] These situations of crisis have aptly been called 'critical moments' in the sociological literature on disputes.[66]

In the case of cryptocurrencies, these critical moments arise when there is a need for a change of the code protocol that governs transactions on the blockchain. The protocol of each

---

[56] Arthur Gervais et al., 'Is Bitcoin a Decentralized Currency?' (2014) 12(3) IEEE Security & Privacy 54; Rainer Böhme et al., 'Bitcoin: Economics, Technology, and Governance' (2015) 29 The Journal of Economic Perspectives 213; Angela Walch, 'The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk' (2015) 18 NYU J Legislation and Public Policy 837, 865-882; id., 'The Fiduciaries of Public Blockchains' Working Paper (2017) (on file with author); Paech (n 55) 18-31 and 42-54; Primavera De Filippi and Benjamin Loveluck, 'The invisible Politics of Bitcoin: Governance crisis of a decentralised Infrastructure', 5(3) Internet Policy Review 1 (2016); Don Tapscott and Alex Tapscott, *Blockchain Revolution* (Penguin, 2016) ch 11; id., 'Realizing the Potential of Blockchain' World Economic Forum White Paper (2017).
[57] See above (n 43).
[58] Tom Simonite, Bitcoin Isn't the Only Cryptocurrency in Town, MIT Tech. Review (April 15, 2013), https://www.technologyreview.com/s/513661/bitcoin-isnt-the-only-cryptocurrency-in-town/.
[59] See references above (n 9).
[60] Bitcoin currently has a market capitalization of more than $121 bio.; Ethereum of more than §31 bio., see https://coinmarketcap.com/ (accessed on 15 November, 2017).
[61] The Swiss region of Zug, for example, even accepts Bitcoin as legal tender to pay tax: Lutz Reiche, 'Steuern zahlen mit Bitcoins - die Schweiz prescht vor' (*Manager Magazin*, May 10, 2015), http://www.manager-magazin.de/finanzen/artikel/bitcoin-zug-akzeptiert-das-cyber-geld-als-zahlungsmittel-a-1091646.html; furthermore, a number online shops already accept cryptocurrencies, see European Central Bank (n 51) 16-17.
[62] See Hacker/Thomale (n 2); Rohr/Wright (n 2)
[63] See, e.g., Eric Brousseau et al. (eds), *Governance, Regulation and Powers on the Internet* (CUP, 2012).
[64] Jeanette Hofmann et al., 'Between coordination and regulation: Finding the governance in Internet governance' (2016) *New Media and Society* 1, 10.
[65] ibid 9.
[66] Luc Boltanski and Laurent Thévenot, 'The Sociology of Critical Capacity' (1999) 2 European Journal of Social Theory 359.

blockchain-based organization specifies exactly how certain transactions are executed, how new coins are created, at what speed the chain is updated, etc. Protocol changes thus alter the "rules of the game" according to which transactions can be accomplished and the system functions. As the following brief case studies will show, imperfect governance structures become particularly visible in the process leading to major breaks in the protocol structure, so-called hard forks.[67]

What is perhaps most striking about the constructive feature of cryptocurrencies is not the high degree of specification in *applying* the protocol to transactions, but the opacity and informality when it comes to the *updating* of the protocol itself.[68] There are no clear guidelines in place describing how the protocol itself can be changed, particularly when conflicting views have to be reconciled.[69] In stark contrast to the exactness of the protocol itself, governance mechanisms are thus almost entirely lacking when it comes to changing the rules of the game in moments of dispute.

In line with complexity theory, the development of the protocol over time can be described as non-linear, interactive, and feedback-driven: a change to the protocol is often driven by user feedback provided on forums and blogs.[70] Besides user feedback, however, there is also a central steering element that has become increasingly apparent in the recent development of cryptocurrencies.

For example, the reference implementation of the Bitcoin protocol, openly accessible at the code platform Github, is maintained by a small group of people ("core developers").[71] While anyone may make proposals for updating the code, only the core developers have the power to actually implement changes.[72] Nonlinearity and unpredictability in changes to the protocol arguably result from the lack of a procedure to accommodate dissent within the community of developers and, more broadly, of users and stakeholders.[73] Core developers use "informal processes that depend on rough notions of consensus and that are subject to no fixed legal or organizational structure".[74] They do, however, often coordinate their actions with operators of

---

[67] While soft forks are reversible and essentially implement changes to the protocol via voluntary software updates (just like updates for other computer programs), hard forks are irreversible and forced upon user communities by mandatory updates. The change in the protocol is so important that users not implementing the novel update are unable henceforth to use the program altogether. Cf. Ofir Beigel, 'Segwit vs. Bitcoin Unlimited and Bitcoin's Fork Explained Simply' (*99 Bitcoins*, March 27/April 2, 2017), https://99bitcoins.com/bitcoin-fork-segwit-vs-bitcoin-unlimited-explained-simply/; https://en.bitcoin.it/wiki/Softfork; Antonopoulos (n 41) 199-204.

[68] On the difference between these two governance layers, see De Filippi and Loveluck (n 56) 10.

[69] Cf. De Filippi and Loveluck (n 56) 14.

[70] Gervais et al. (n 56) 55; https://github.com/bitcoin/bips/blob/master/README.mediawiki.

[71] Cf. Dwyer (n 45) 82; Gervais et al. (n 56) 55.

[72] Gervais et al. (n 56) 57; De Filippi and Loveluck (n 56) 13-14; Angela Walch, 'The Fiduciaries of Public Blockchains' Working Paper (2017) (on file with author) 5: only core developers have the "commit key".

[73] The core developers note: "We are fairly liberal with approving BIPs [Bitcoin Improvement Proposals], and try not to be too involved in decision making on behalf of the community. The exception is in very rare cases of dispute resolution when a decision is contentious and cannot be agreed upon. In those cases, the conservative option will always be preferred." https://github.com/bitcoin/bips/blob/master/README.mediawiki (accessed on June 8, 2017).

[74] Shawn Bayern, 'Of Bitcoins, Independently Wealthy Software, and the Zero Member LLC' (2014) 108 Nw. U. L. Rev. Online 257, 259.

large mining pools;[75] these are entities that supply the computing power to validate transactions in the chain and that are rewarded for their efforts with newly "minted" coins.[76] A small group of agents crucial for the development and maintenance of the network (core developers and operators of mining pools) may thus acquire true power to change the protocol, even when holding less than 50 % of computing power,[77] and independent of their financial stakes in the currency. While these agents effectively regulate the crypto-economy, they are accountable to no-one, and users do not play any significant role in their appointment.[78]

3. Case Studies

We shall now take a look at three specific examples: two hard forks by Bitcoin and Ethereum, which happened in March 2013 and July 2016, respectively; and the controversy surrounding the bitcoin scaling debate which has led to yet two more hard forks in 2017, driven by disagreement over updating the rules on block sizes.

a) The Bitcoin Hard Fork of 2013

On March 11, 2013, the Bitcoin blockchain forked into two chains that were no longer mutually consistent.[79] This unintended hard fork was a result of slow updating to the newly released version of the protocol. Importantly, the new chain was growing faster than the old one. However, the core developers convinced the largest mining pool (BTC Guild)[80] and other major pools via the bitcoin-dev IRC channel,[81] without any coordination with users, to back the shorter chain because it functioned under both old and new versions.[82] In doing so, they violated the basic blockchain rule of the authenticity of the longest chain.[83] Thanks to the efforts of the mining pools which controlled roughly 70 % of the hash power of the Bitcoin network, the shorter, old chain caught up and eventually surpassed the new chain.[84] Mining rewards worth 26,000 $ in the new chain were lost, and 10,000 $ double spent as a result of the fork.[85] In this case, therefore, the operators of major mining pools and core developers informally colluded to take the blockchain into a novel, non-majoritarian, direction. While their intentions to quickly resolve the fork may have been laudable, the episode shows the vulnerability of the infrastructure to *ad hoc* coalitions of the willing.

---

[75] See Angela Walch, 'The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk' (2015) 18 NYU J Legislation and Public Policy 837, 873.
[76] See Antonopoulos (n 41) 207-210.
[77] Gervais et al. (n 56) 55.
[78] Gervais et al. (n 56) 55.
[79] Gervais et al. (n 56) 56.
[80] Arvind Narayanan, Analyzing the 2013 Bitcoin fork: centralized decision-making saved the day https://freedom-to-tinker.com/blog/randomwalker/analyzing-the-2013-bitcoin-fork-centralized-decision-making-saved-the-day/, introductory section, and under Achtung !.
[81] http://bitcoinstats.com/irc/bitcoin-dev/logs/2013/03/11.
[82] Gervais et al. (n 56) 56; Buterin (n 45).
[83] As a maximum, the new chain was 13 blocks ahead: Buterin (n 45).
[84] Buterin (n 45).
[85] Buterin (n 45); the transactions in the lost blocks of the new chain, however, were later added to the dominant, old chain so that they could be executed.

b) The Ethereum Hard Fork of 2016

In this way, even transaction histories may be changed retroactively, sacrificing a second basic rule of blockchain: its irreversibility.[86] This is exactly what happened on July 20, 2016 in the Ethereum blockchain, a younger blockchain which not only defines a cryptocurrency (ether) but also enables smart contracts.[87] As mentioned, Ethereum is also configured to support networks of smart contracts known such as token-based ventures.[88] These decentralized applications can take a broad variety of forms. In the specific instance, a German startup programmed a smart contract running on Ethereum called "The DAO" which was intended to function like a decentralized investment platform. Having collected a surprising equivalent of 150 million dollars in ethers, representing 15% of all outstanding ether, The DAO was hacked and deprived of a third of its funds.[89] Overnight, ethers lost half of their value.[90]

In an unprecedented move, core Ethereum developers decided to effectively rewrite the history of their blockchain in order to undo the hack and restore the funds to all investors via a hard fork.[91] This process is unique in so far as the blockchain, which is supposed to be an irreversible record of all transactions, was changed in order to erase the consequences of the fundamental coding error which led to the greatest hack in the history of blockchain-based organizations.[92] The proposers of this rewriting of the Ethereum blockchain subjected their radical ideas to the majority vote of users by conditioning the hard fork on the approval by the majority of users.[93] The proposal was fiercely contested.[94] Only a minority of ether owners voted,[95] but in the end, the vast weighted majority of those users that did vote[96] and, after this, a similar majority of computing power of miners backed the hard fork.[97] Other than in the case of the unintentional Bitcoin fork just discussed, the intentional Ethereum fork was thus subjected to a dual mechanism: first, a vote by users, and then, the (unavoidable and economic) vote of miners by virtue of their computing power, who decided on whether to back the old or the newly forked

[86] See, on rewriting blockchain history, David Siegel, 'Understanding The DAO Attack' (*Coindesk*, June 25, 2016), http://www.coindesk.com/understanding-dao-hack-journalists/.
[87] Joon Ian Wong and Ian Klar, 'Everything you need to know about the Ethereum "hard fork"' (*Quartz*, July 18, 2016), http://qz.com/730004/everything-you-need-to-know-about-the-ethereum-hard-fork/.
[88] Vitalik Buterin, 'Ethereum White Paper' (2014).
[89] Siegel (n 86); Wong and Klar (n 87).
[90] Luke Parker, 'Ethereum hard fork results in two surviving cryptocurrencies, both are now trading' (*Brave New Coin*, July 26, 2016) https://bravenewcoin.com/news/ethereum-hard-fork-results-in-two-surviving-cryptocurrencies-both-are-now-trading/.
[91] The ethers originally collected in The DAO, which had then siphoned off to a child DAO by the attacker and to yet another DAO by friendly hackers (white hats), were restored to a WithdrawDAO recovery contract. The token holders can reclaim their investments in this way. See Jeffrey Wilke, 'To fork or not to fork' (*Ethereum Blog*, July 15, 2016), https://blog.ethereum.org/2016/07/15/to-fork-or-not-to-fork/.
[92] See above (n 86).
[93] The vote was weighted by the ethers of the users, http://carbonvote.com/; see also Wilke (n 91).
[94] See, e.g.: "To me [the hard fork] is totally unacceptable and is a departure from the principles that drew me to ethereum." (user "nustiudinastea", posted on https://www.reddit.com/r/ethereum/comments/4oiqj7/critical_update_re_dao_vulnerability/ (June 2016).
[95] Walch (n 72) 7; Parker (n 90).
[96] In the end, 87 % supported the hard fork: Parker (n 90).
[97] Already on June 20, 2016, 85 % of miners were mining on the new fork: Vitalik Buterin, 'Hard Fork Completed' (*Ethereum Blog*, July 20, 2016), https://blog.ethereum.org/2016/07/20/hard-fork-completed/.

version.[98] Nevertheless, in a way difficult to foresee ex ante, the principle of the immutability of the chain was sacrificed.

c) Bitcoin Hard Forks without End: The Ongoing Block Size Debate

The ongoing controversy over the best way to fix a problem inherent in the current Bitcoin implementation provides a third example of potentially complex and unpredictable behavior. Even after two hard forks in August and October 2017, creating Bitcoin Cash[99] and Bitcoin Gold,[100] the Bitcoin network is still facing its probably largest challenge for a stable and sustainable future: the scaling debate.[101] With its current configuration, the Bitcoin blockchain can only validate a limited number of transactions per block.[102] This prompted Bitcoin Cash to raise the block size to 8 MB. However, the block size of the legacy Bitcoin chain is still capped at 1 MB. The community is fiercely split over the question whether, and to what extent, to raise this limit.

The most notable implementation that would achieve increased block size is called Segregated Witness (SegWit). Without going into the details,[103] it is safe to say that the proposal that came closest to adoption, called SegWit2x, would have freed up space for transactions in the blocks and additionally raised the block size to 2 MB. SegWit2x would be have been implemented by a hard fork around November 16 if only enough miners backed it.[104] Observers agreed that, if anything, the threat of a hard fork seeking to take along the majority of the nodes of the legacy Bitcoin chain (and not only open a new chain as Bitcoin Gold and Cash did, respectively), infused significant uncertainty as to the future of the Bitcoin blockchain[105] – again testifying to

---

[98] On the necessary backing by miners, see Wong and Klar (n 87).
[99] Alyssa Hertig, 'Bitcoin Cash: Why It's Forking the Blockchain And What That Means' (*CoinDesk*, July 26, 2017), https://www.coindesk.com/coindesk-explainer-bitcoin-cash-forking-blockchain/.
[100] Alyssa Hertig, 'Bitcoin Gold: What to Know About the Blockchain's Next Split' (*CoinDesk*, October 23, 2017), https://www.coindesk.com/bitcoin-gold-know-blockchains-next-split/.
[101] See, e.g., Ofir Beigel, 'Segwit vs. Bitcoin Unlimited and Bitcoin's Fork Explained Simply' (*99 Bitcoins*, March 27/April 2, 2017), https://99bitcoins.com/bitcoin-fork-segwit-vs-bitcoin-unlimited-explained-simply/; Pete Rizzo, 'Making sense of Bitcoin's divisive block size debate' (*CoinDesk*, January 19, 2016), http://www.coindesk.com/making-sense-block-size-debate-bitcoin/; De Filippi and Loveluck (n 56) 7-9; CoinDesk, 'Bitcoin or Bitcoin2x? News & Guides to Navigate November's Fork' (*CoinDesk*, October 30, 2017).
[102] Arvind Narayanan et al., 'Bitcoin and Cryptocurrency Technologies. A Comprehensive Introduction' (Princeton University Press, 2016) ch 3.6 and 7.
[103] For an excellent technical introduction, see Aaron van Wirdum, 'Segregated Witness, Part 1: How a Clever Hack Could Significantly Increase Bitcoin's Potential' (*Bitcoin Magazine*, December 19, 2015), https://bitcoinmagazine.com/articles/segregated-witness-part-how-a-clever-hack-could-significantly-increase-bitcoin-s-potential-1450553618/.
[104] Pete Rizzo, 'Understanding Segwit2x: Why Bitcoin's Next Fork Might Not Mean Free Money' (*CoinDesk*, November 1, 2017), https://www.coindesk.com/understanding-segwit2x-bitcoins-next-fork-might-different/.
[105] CoinDesk (n 101): "it remains unclear whether the new code will change bitcoins' rules, or if another new cryptocurrency will be created"; Laura Shin, 'Will This Battle For The Soul Of Bitcoin Destroy It?' (*Forbes*, October 23, 2017), https://www.forbes.com/sites/laurashin/2017/10/23/will-this-battle-for-the-soul-of-bitcoin-destroy-it/#c3f4e323d3c0; Pete Rizzo, 'Split or No Split? Bitcoin Miners See No Certainty in Segwit2x Fork' (*CoinDesk*, November 1, 2017), https://www.coindesk.com/split-no-split-bitcoin-miners-see-no-certainty-segwit2x-fork/; Ariel Deschapel, 'Why Segwit2x Is Doomed to Fail' (*CoinDesk*, November 6, 2017), https://www.coindesk.com/opinion-segwit2x-doomed-fail/, under "Scheduled chaos": "The almost nine-year-old cryptocurrency is facing its gravest test yet. Whether or not it will survive, or in what form, is anyone's guess."; Rizzo (n 104).

its complex nature. Further complicating matters, the SegWit2x hard fork was called off at the last minute,[106] leaving users and app developers perplexed about the future of scaling on the Bitcoin blockchain.[107]

The SegWit2x scaling proposal sounds familiar to Bitcoin followers: throughout the last year, parts of the community have argued for an adaptable, theoretically unlimited block size that would primarily be driven by current demand (called the Bitcoin Unlimited solution).[108] Before, Bitcoin XT, pitted against the legacy Bitcoin Classic/Core, offered similar promises of greater block size,[109] and deeply divided the community.[110] Supporters of each threatened to implement their vision by a hard fork from the traditional Bitcoin blockchain. As noted, Bitcoin Cash was also motivated by the desire to raise the block size limit, but in ways different from SegWit.[111]

Arguably, however, all solutions enable, through different avenues, the steering of the bitcoin currency by informal, already powerful groups. A greater block size would make it more difficult for conventional computers to process transactions in the first place, making those with significant computing power even more relevant.[112] As in the case of Bitcoin Unlimited, there was a growing fear that under SegWit2x control would be effectively handed over to mining pool operators.[113] Unsurprisingly, miners, and not users, were the only ones able to cast votes on whether SegWit2x would be adopted.[114]

Many users and, notably, the Bitcoin core developers therefore opposed the SegWit2x proposal.[115] However, the alternative is also all but devoid of power problems. Earlier in 2017, the core developers held meetings with large mining pool operators, for example in China, to

---

[106] Alyssa Hertig, '2x Called Off: Bitcoin Hard Fork Suspended for Lack of Consensus' (*CoinDesk*, November 8, 2017), https://www.coindesk.com/2x-called-off-bitcoin-hard-fork-suspended-lack-consensus/.

[107] Pete Rizzo and Alyssa Hertig, 'Relief and Disbelief: Bitcoin Reacts to Sudden '2x' Suspension' (*CoinDesk*, November 8, 2017), https://www.coindesk.com/relief-disbelief-bitcoin-reacts-sudden-2x-suspension/.

[108] Frisco d'Anconia, 'Roger Ver Defends Bitcoin Unlimited, Says Core Deviated' (*Cointelegraph*, April 17, 2017).

[109] Daniel Palmer, 'Scalability debate continues as Bitcoin XT proposal stalls' (*CoinDesk,* January 11, 2016), http://www.coindesk.com/scalability-debate-bitcoin-xt-proposal-stalls; De Filippi and Loveluck (n 56) 8 et seq.

[110] Mike Hearn, 'The resolution of the Bitcoin experiment' (*Mike's blog*, January 14, 2016), https://blog.plan99.net/the-resolution-of-the-bitcoin-experiment-dabb30201f7.

[111] Josiah Wilmoth, 'The First 8MB Bitcoin Cash Block Was Just Mined' (*CryptoCoinsNews*, August 17, 2017), https://www.cryptocoinsnews.com/first-8mb-bitcoin-cash-block-just-mined/.

[112] De Filippi and Loveluck (n 56) 8; Rizzo (n 104).

[113] Don Tapscott and Alex Tapscott, 'Realizing the Potential of Blockchain' World Economic Forum White Paper (2017), 11; Beigel (n 101).

[114] This is due to the use of the BIP 9 activation protocol, see Matthew Haywood, 'All roads lead to Segwit—Segwit2x, BIP 91 Segsignal and UASF' (*Medium*, July 24, 2017), https://medium.com/@wintercooled/segwit2x-segsignal-and-the-uasf-all-roads-lead-to-segwit-d66fedf7fba; Rizzo (n 104); Alyssa Hertig, 'Why Are Miners Involved in Bitcoin Code Changes Anyway?' (*CoinDesk,* November 1, 2017), https://www.coindesk.com/miners-involved-bitcoin-code-changes-anyway/; critique also in Deschapel (n 105), under "A flawed outlook".

[115] Alyssa Hertig, 'Bitcoin 'Battle'? Core Developers Apathetic as Segwit2x Fork Approaches' (*CoinDesk,* November 1, 2017), https://www.coindesk.com/bitcoin-battle-developers-apathetic-segwit2x-fork-approaches/; Rizzo (n 104).

discuss possible solutions, raising the fear of collusion between the groups.[116] Core developers have also been accused of illegitimate censorship in the scaling debate.[117]

Again, it appears that a small group of technological leaders (miners, core developers) tries to leverage their position, assume informal power and, in opaque ways, influence the decision about the updating of the protocol. It was precisely this tendency that sparked the hard fork generating Bitcoin Gold, which aims to restore user power,[118] but has been dwarfed by the legacy Bitcoin chain in importance so far.[119]

d) Lessons from the Hard Forks

In all cases just discussed, a clear imperfection of governance schemes becomes apparent. It allows for the coordinated actions of a few major stakeholders or developers to take control of the rules for constructing the blockchain. Of course, any person can make changes to the open source software and thereby launch a new cryptocurrency. However, the important question is who is deciding on the development of the existing, successful currencies (such as bitcoin or ethereum), in which users or investors have already acquired substantial amounts of coins. The three examples show that the decentralized structure is vulnerable to coalitions of the willing, which combine enough technological prowess, computing power, or force of persuasion to implement their proposals on the development of the blockchain.[120] This leads to erratic, unforeseen and potentially radical changes of the system status as a reaction to external shocks or internal developments. This is exactly the kind of behavior that complexity theory predicts for complex systems.

4. Complexity and Cryptocurrencies

All in all, the case studies show that cryptocurrencies possess five properties that suggest they qualify as complex systems. First, a great degree of heterogeneity between the actors exists, in terms of their tech-savviness, rationality, motivations, and goals. Second, they exhibit a clear network character, being based on decentralized nodes. Third, the lack of altering rules for the blockchain protocols, and the concomitant lack of governance schemes to deal with dissent, unforeseen events or security breaches, leads to an inherent unpredictability of the future development of the protocols when coalitions of major players (core developers, operators of mining pools) can exert disproportionate power to unilaterally push updates they view as personally favorable or generally reasonable. Fourth, this abstract lack of governance has manifested itself in a series of concrete events in which major transitions in the protocol were conducted. This included the violation of perhaps the two most basic rules of blockchain, namely the invalidation of the significantly longer chain, and the entire rewriting of the blockchain by erasure of an investment vehicle worth more than 150 Mio. $. Finally, the value of cryptocoins is so volatile that some economists tend to categorize cryptocurrencies as

[116] JP Buntinx, 'Bitcoin Core Members Discuss Blockchain Consensus At Chinese Event' (*The Merkle*, December 11, 2016), https://themerkle.com/bitcoin-core-members-discuss-blockchain-consensus-at-chinese-event/; Walch (n 72) 9.
[117] John Blocke, '/r/Bitcoin Censorship, Revisited' (*Medium*, February 27, 2017), https://medium.com/@johnblocke/r-bitcoin-censorship-revisited-58d5b1bdcd64.
[118] See BitcoinGold, 'Roadmap', https://bitcoingold.org/.
[119] See CoinMarketCap, 'Bitcoin Gold [Futures]', https://coinmarketcap.com/currencies/bitcoin-gold/ (accessed on November 6, 2017).
[120] Cf. Dwyer (n 45) 82.

investment assets rather than currencies.[121] Price volatility, however, is another instantiation of unpredictable behavior exhibited by complex systems.[122]

The upshot of treating cryptocurrencies as complex systems is threefold. First, on the predictive level, if the analysis is correct, we should expect to see more unpredictable behavior over time; this implies radical uncertainty for cryptocurrencies and token-based ventures built on top of them. Second, on the descriptive level, specific complexity analyses (e.g., agent-based models[123]) may better match the actual behavior of the system than traditional economic analysis, and help predict transitions from stable to unstable states.[124] Third, on the normative level, regulation should strive to strengthen elements of order and reduce uncertainty in the development of the system by tackling, where possible, the roots of complexity and unpredictability. This is precisely what the final part of the article is about.

IV. Regulating Blockchain-Based Organizations under Uncertainty

Complexity implies uncertainty concerning the future development of a system. Against this background, regulation can arguably take two different approaches: first, regulation may take uncertainty as given and attempt to *accommodate* it, e.g. through principles-based regulation;[125] second, it may *reduce* uncertainty by installing institutional frameworks. This paper takes the second approach: it suggests that uncertainty may be reduced, and elements of order strengthened, by the implementation of governance mechanisms. In this, it draws primarily on a comply or explain approach, which promises to cure the ills of re-centralization in blockchain-based systems while respecting the freedom to innovate and experiment.

1. Mitigating Uncertainty: Improving Governance Structures in Blockchain-Based Organizations

David Yermack has shown, in an influential paper, how blockchain technology stands to uproot corporate governance mechanisms;[126] however, the inverse question of the adaptability of corporate governance rules to blockchain applications like cryptocurrencies has not yet been posed. The remainder of the article sets out to fill this gap. Core developers and important miners wield powers that are comparable with those of the management of publicly traded companies; however, they are not subject to the same rules of scrutiny, transparency and accountability faced by company managers. Cryptocurrency governance rules could change that.

---

[121] Cheah and Fry (n 15) 33; David Yermack, 'Is Bitcoin a Real Currency: An Economic Appraisal' in David Lee Kuo Chuen (ed) *Handbook of Digital Currency* (Elsevier 2015) 31, 32; Dirk G Baur et al., 'Bitcoin: Currency or Investment?' Working Paper (2014), https://ssrn.com/abstract=2561183.
[122] Cheah and Fry (n 15) 35; Battiston et al. (n 1) 819.
[123] See, e.g., Blake LeBaron, 'Agent-Based Computational Finance' in Leigh Tesfatsion and Kenneth L. Judd (eds) *Handbook of Computational Economics*, Volume 2 (North-Holland, 2006) 1187.
[124] Stefano Battiston et al. (n 1) 818 (see also n. 2 there).
[125] See, e.g., Julia Black, 'Forms and paradoxes of principles-based regulation' (2008) 3 *Capital Markets Law Journal* 425.
[126] David Yermack, 'Corporate Governance and Blockchains' (2017) 21 Review of Finance 7; see also Wright and De Filippi (n 47) 31 and 36-37.

a) Reasons to Improve Governance through Legal Intervention

There are six reasons that speak in favor of the installation of concrete governance mechanisms for cryptocurrencies in general, and for drawing on corporate governance in particular. First, in general, governance mechanisms may rein in, to a certain extent, the spontaneous, uncoordinated and unpredictable interaction of users and other stakeholders. Therefore, they can produce a shift from complexity towards a greater degree of order in the system, strengthening regularity and stability. This would likely be appreciated not only by most current users but also by potential future users, who at the moment refrain from getting involved with cryptocurrencies precisely because of the described governance problems. It also protects third parties from ripple effects that are likely to become larger as cryptocurrencies gain market capitalization. Therefore, second, the introduction of governance rules takes the first steps towards a shift in the legal perspective on cryptocurrencies: from currency regulation to investor protection. This is particularly relevant in the context of novel tokens born out of ICOs that are, more often than not, perceived as investment opportunities by their holders.[127] As mentioned, economists have argued that, given their volatility, cryptocurrency tokens should be treated like investment assets and not like pieces of electronic currencies.[128] While this debate cannot be decided in this article, it seems clear that at least some suitable measures of investor protection should be implemented to safeguard the interests of cryptocoin owners against those of other, more powerful stakeholders. Third, a clear designation of competences and procedures would break up the informal power structures that hold sway in cryptocurrency systems, and more generally in token-based systems,[129] at the moment, presenting an opportunity to distribute power in a fairer and more transparent way. Fourth, the provision of a governance system by the law solves the collective action problem among users that, arguably, prevents them from lobbying effectively for a governance system themselves.[130]

Fifth, *corporate* governance rules, as we will see in greater detail (see below, Part IV.2.), primarily work through a "comply or explain" approach that delegates ultimate choice about the adoption of good governance rules to the regulated entity: it either has to comply with a Corporate Governance Code, or disclose why it does not comply with it. Most recently, Article 3j of the amended Shareholder Rights Directive[131] has extended the comply or explain approach to proxy advisors that counsel shareholders on their voting decisions. As this regime takes root in financial services, it seems ripe to be transposed to cryptocurrencies and token-based ventures as well. The upshot would be that these systems have the choice not to incur the cost of implementing robust governance structures, and may continue to experiment with minimal ones – if only they adequately and saliently inform the public about this decision. Particularly smaller cryptocurrencies or token projects may therefore selectively opt out of the entire Blockchain Governance Code, or out of parts of it that they find disproportionately

[127] See Adhami et al. (n 127), 'Why Do Businesses Go Crypto? An Empirical Analysis of Initial Coin Offerings', Working Paper (20 October, 2017), https://ssrn.com/abstract=3046209, at 21; more generally, Hacker/Thomale (n 2); Rohr/Wright (n 2).
[128] See above (n 121.
[129] See above (n 11).
[130] On collective action problems in large groups, see, e.g., Mancur Olson, *The Logic of Collective Action* (Harvard University Press 1965); Elinor Ostrom, 'A Behavioral Approach to the Rational Choice Theory of Collective Action' (1998) 92 American Political Science Review 1.
[131] Directive (EU) 2017/828 of the European Parliament and of The Council of 17 May 2017 amending Directive 2007/36/EC as regards the encouragement of long-term shareholder engagement, OJ 2017 L 132/1 (henceforth SRD).

burdensome.[132] This framework therefore balances incentives for technical experimentation with user protection; mandatory governance rules, by contrast, should only be considered for those cryptocurrencies, or token-based ventures, that have gained significant importance in the financial system (see below, section IV.2.c)).

Sixth, it is currently often unclear which state(s)' law applies to cryptocurrencies, or token-based projects.[133] An empirical study has found that users do appreciate a clear choice of a reference jurisdiction in token sales.[134] The elaboration of a Blockchain Governance Code would partially solve this problem: it would contain a minimal set of rules that applies to a cryptocurrency that adopts it. By implication, the governance framework for cryptocurrencies, other than national Corporate Governance Codes, has to be developed with an international reach so that it can apply to blockchain-based projects with core developers, miners and users scattered across the globe.[135] Drawing extensively on corporate governance, the next sections spell out what such a framework might look like.

b) External and Internal Governance: From Corporate to Crypto

Spurred on by the corporate scandals and board room abuses of the 1980s,[136] the literature on corporate governance analyzes the optimal structure for decision making within companies.[137] It distinguishes between external and internal governance,[138] mirroring Albert Hirshman's distinction between exit and voice.[139]

1) The Corporate Framework

External governance is concerned with optimizing parameters that lie outside the company itself but that nevertheless have a decisive impact on managerial decision making within the company. Shareholders can sell their shares on the market (exit).[140] Thereby, shareholders may divest from a company they perceive to be badly managed. Moreover, importantly, the market for shares offers those seeking to take over a target company a way to buy a sufficient number of shares to oust the current management and install a new one. External governance therefore is

---

[132] Cf. Financial Reporting Council, UK Corporate Governance Code (June 2016), https://www.frc.org.uk/Our-Work/Codes-Standards/Corporate-governance/UK-Corporate-Governance-Code.aspx [UK CGC] para 5.
[133] See Iris M. Barsan, 'Legal Challenges of Initial Coin Offerings (ICO)' (2017)(3) *RTDF* 54, 63 et seqq.
[134] Adhami et al. (n 127) 21 et seq.
[135] On the legal issues surrounding the regulation of cross-jurisdictional blockchain-based networks, see Paech (n 55) 46-54.
[136] R I (Bob) Tricker, The Evolution of Corporate Governance in Thomas Clarke and Douglas Branson (eds) *The SAGE Handbook of Corporate Governance* (SAGE 2012) 39, 44-45.
[137] Stefan Grundmann, *European Company Law* (2d edn, Intersentia 2012) § 14 para. 1; cf. also Thomas Clarke and Douglas Branson, 'Introduction: Corporate Governance – And Emergent Discipline?' in id. (eds) *The SAGE Handbook of Corporate Governance* (SAGE 2012) 1, 2-3.
[138] Grundmann (n 137) § 14 para. 11.
[139] Albert O Hirschman, Exit, voice, and loyalty: Responses to decline in firms, organizations, and states (Harvard University Press 1970).
[140] Grundmann (n 137) § 14 para. 35-36; 40-42.

fundamentally linked to the market for corporate control, which in turn exerts pressure on current management to satisfy shareholder demands lest it be replaced in a hostile takeover.[141]

Internal governance, by contrast, describes channels of influence by which shareholders can discipline the management (voice).[142] It comprises information rights, approval rights (for example, since recently in the EU, a say on pay, Art. 9a, b SRD), and the core competence of the general meeting of shareholders to decide on fundamental matters pertaining to the company.[143] More generally, internal governance formulates a regime for a balance of power between different organs of the company (board of directors, shareholders, supervisory board where applicable).

2) The Comparability of Corporations and Blockchain-Based Organizations

Turning to blockchain, it may at first glance seem far-fetched to compare informal, open source-based networks of agents in a cryptocurrency system with the highly formalized processes involved in corporations. This difference is most pronounced, however, on a certain theoretical rather than on a practical level. It is true that orthodox corporate governance is built on principal agency or stewardship theory,[144] i.e., theories that presuppose a hierarchically structured company.[145] These theoretical foundations seem to be at odds with less hierarchical, network-type organizations such as cryptocurrencies or decentralized applications.[146] Nevertheless, the comparison is useful for four reasons. First, as the case studies have shown, abuses of power by a subgroup of actors can be detected within cryptocurrencies – as mentioned, similar incidents led to corporate governance rules in the 1980s. Second, both entities (corporations and cryptocurrency systems) have to overcome the challenge of coordinating, and stabilizing, the behavior of a wide range of actors, some of whom assume – informally or formally – a centralizing management function (directors and core developers/potentially large miners) while others are rather diffused and may suffer from collective action problems (shareholders and cryptocoin owners). Despite the theoretically flat hierarchies of cryptocurrency networks, the case studies have shown that a *de facto* separation between ownership (of cryptocoins) and control (over protocol changes) exists – precisely like in publicly traded companies.[147] Third, as scholars have pointed out, the grounding of governance questions in human decision making which, in turn, is universally limited by cognitive capacity constraints, make non-hierarchical and hierarchical organizations comparable from a governance perspective:[148] both types of organization need to separate tasks, and power, in order to prevent information overload of their members.[149] Fourth, tokens issued in token sales function not only as decentralized means of payment, but even more so as alternative routes for financing entrepreneurial projects that,

---

[141] Henry G Manne, 'Mergers and the Market for Corporate Control' (1965) 73 Journal of Political Economy 110.
[142] See Bob Tricker, *Corporate Governance* (2d ed., OUP 2012) 86-88.
[143] Julian Velasco, 'Taking Shareholder Rights Seriously' (2007) 41 UC Davis L. Rev. 605.
[144] Tricker (n 136) 53-57.
[145] Shann Turnbull, 'The Limitations of Corporate Governance Best Practices' in Thomas Clarke and Douglas Branson (eds) *The SAGE Handbook of Corporate Governance* (SAGE 2012) 428, 434.
[146] Turnbull (n 145) 434; see also David Craven et al., 'New Organizational Forms for Competing in Highly Dynamic Environments: the Network Paradigm' (1996) 7 British Journal of Management 203.
[147] Eugene F. Fama and Michael C. Jensen, 'Separation of Ownership and Control' (1983) 26 The Journal of Law and Economics 301.
[148] Turnbull (n 145) 435.
[149] Shann Turnbull, *A New Way to Govern: Organisations and Society After Enron* (New Economics Foundation Pocketbook 2002) 5-6.

outside of the blockchain, would require the foundation of traditional companies.[150] Many of these for-profit token applications, therefore, share a number of characteristics with companies, or even investment funds, rather than with open-source networks. Hence, it has even been suggested that blockchain-based networks might, in themselves, be partnerships in a legal sense, particularly if users follow a joint purpose and share profits;[151] this reasoning would apply *a fortiori* to token systems launched by ICOs, particularly to investment tokens.[152]

Therefore, many of the problems corporate governance is supposed to solve reappear in cryptocurrency and decentralized application regimes. It is clear, however, that in the adaptation of corporate governance concepts to cryptocurrencies, we have to take account not only of the similarities, but also of the profound differences between these entities.

3) The Blockchain Governance Framework

To start with, we may also distinguish between an external and an internal governance perspective in the realm of cryptocurrencies and token-based ventures.[153] Concerning the external dimension, an analogy to a market for corporate control does not exist at the moment. There is no formal way to oust the core developer team by means of a “takeover”. The introduction of such a feature by legal means would indeed provide a strong, disciplining incentive for core developers to act reasonably and in the interest of users. However, the technical specificities of each blockchain make it difficult to replace an entire core developer team. The difficulties of the developers of Bitcoin Unlimited to implement a version of their alternative cryptocurrency that is free from fundamental bugs testifies to this problem.[154] At this point, it becomes apparent that the cryptocurrency is not simply a company; it is also a financial infrastructure. The introduction of a “market for cryptocurrency control” would likely introduce *more* instability into the valuation and decision making of the currency than mitigate governance problems. While temporarily instable companies can be tolerated easily in a market economy, inherently instable financial infrastructures seem much less desirable. This reason applies less to token-based ventures such as Filecoin or Status that lack a primary financial component; however, it is often difficult to draw the line between those tokens with currency and those with internal utility functions.[155]

Therefore, it is other instruments of external governance that should be pursued in the first place. One exit strategy for users is, of course, the simple sale of their cryptocoins.[156] To the extent that core developers are not directly responsible to users, this option does not exert direct pressure on core developers, only indirectly through the pricing mechanism if enough users sell simultaneously. However, there is another and more potent “exit tool” that is lacking in

---

[150] See references above (n 2 and 12).
[151] Zetzsche et al., ‘The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain’, *U. Illinois L. Rev.* (forthcoming), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3018214, at 36 et seq.; Mann, 'Die Decentralized Autonomous Organization – ein neuer Gesellschaftstyp?', *NZG* 2017, 1014, 1017.
[152] For this terminology, see Hacker/Thomale (n 2); Rohr/Wright (n 2).
[153] See also Ying-Ying Hsieh et al., ‘The Internal and External Governance of Blockchain-Based Organizations: Evidence from Cryptocurrencies’ in: Campbell-Verduyn (ed.), *Bitcoin and Beyond: Blockchains and Global Governance* (Routledge, forthcoming), https://ssrn.com/abstract=2966973.
[154] Garrett Keirns, ‘Bitcoin Unlimited Nodes Recover After Second Bug Exploit’ (*CoinDesk*, March 23, 2017), http://www.coindesk.com/bitcoin-unlimited-releases-bug-patch-as-exploit-brings-down-nodes/.
[155] Hacker/Thomale (n 2) Part IV.B.1.b.ii.(5)(ii).
[156] See, for the selling shares as a corporate governance instrument, Grundmann (n 137) § 14 para. 50.

corporate governance: the possibility to initiate a hard fork at any time.[157] Since cryptocurrencies are based on open source software, anybody can create an alternative currency that resembles the original one but changes a set of rules that users were discontented with.

However, as we have seen, unregulated hard forks create the very uncertainty that ought to be reduced. Therefore, a key challenge to external cryptocurrency governance is the development of a meaningful regime for hard forks; it must strike the difficult balance between safeguarding users' rights to exit with mitigating destabilizing consequences for those remaining with the original version of the cryptocurrency.[158]

Internal governance mechanisms, by contrast, give a voice to users; most importantly, they would therefore clearly establish community referenda on fundamental matters pertaining to the cryptocurrency or token-based venture. These may comprise, for example, the violation of basic rules of public blockchains; hard forks; and other matters of vital interest to users. The next section will spell out in greater detail how such external and internal governance mechanisms could be implemented within the framework of existing cryptocurrencies and decentralized applications.

2. Implementation: The Blockchain Governance Code

Arguably, the greatest innovation in the theory and practice of corporate governance since the 1990s has been the elaboration of Corporate Governance Codes.[159] Often drafted by expert panels, these model codes were first produced as advisory reports whose corporate implementation was largely voluntary[160] (self-regulation[161]). Only gradually were they turned into Codes, with the UK taking the lead, accompanied by the mentioned comply or explain requirement (co-regulation): companies had to either adhere to the Codes or explain to what extent and why they didn't.[162] Codes have since expanded across the globe into virtually all industrialized nations;[163] at the European level, the European Commission also soon recognized them as an effective tool for steering corporate governance through comply or explain. Hence, Art. 46a of Directive 2006/46/EC mandated this approach for listed companies in the EU.[164] In recent years, comply or explain has been extended to a number of fields such as say on pay, insider trading, corporate takeover and rating agency regulation.[165] Most recently, Art. 3j SRD has stipulated such requirements for proxy advisors, as has already been noted.[166]

---

[157] Cf. Linus Nyman and Juho Lindman, 'Code forking, governance, and sustainability in open source software' (2013) 3 Technology Innovation Management Review 7.
[158] See below, Part IV.2.a)6).
[159] Cf. Tricker (n 136) 45.
[160] John Roberts, 'Between the Letter and the Spirit: Defensive and Extensive Modes of Compliance with the UK Code of Corporate Governance' in Thomas Clarke and Douglas Branson (eds) *The SAGE Handbook of Corporate Governance* (SAGE 2012) 196.
[161] Cary Coglianese and Evan Mendelson, 'Meta-Regulation and Self-Regulation' in Robert Baldwin et al. (eds) *The Oxford Handbook of Regulation* (OUP 2010) 146.
[162] Klaus Hopt, 'Comparative Corporate Governance: The State of the Art and International Regulation' (2011) 59 American Journal of Comparative Law 1, 10-11; Tricker (n 136) 45-46.
[163] For an empirical analysis, see Alessandro Zattoni and Francesca Cuomo, 'Why adopt codes of good governance? A comparison of institutional and efficiency perspectives' (2008) 16 Corporate Governance: An International Review 1.
[164] Directive 2006/46/EC of the European Parliament and of the Council of 14 June 2006, OJ 2006 L 224/1 (Annual Accounts Amendment Directive).
[165] Leyens (n 17) 417-419.
[166] See above (n 131).

Admittedly, Corporate Governance Codes have been criticized as ineffective and excessively focused on control and accountability.[167] However, it remains true that the strength of the comply or explain approach lies in offering a "discretionary solution which nevertheless provides transparency".[168] As such, it seems ideally suited for cryptocurrency frameworks that currently lack transparency but that equally ought to preserve opportunities for experimentation and innovation.[169] Particular Codes for specific sectors are well-known, for example for family businesses or partially state-owned companies.[170]

To be effective, however, a Blockchain Governance Code would need to fulfill four conditions: first, the preconditions for the effectiveness of governance codes need to be fulfilled (sub a)). Second, it must contain rules that aim at the solution of the main governance problems that lead to instability in cryptocurrencies (sub b)). Every cryptocurrency, and token-based venture, may then, in principle, choose whether it would like to adopt the code or not. Therefore, third, compliance or non-compliance with the code needs to be disclosed in a cognitively optimized way so that users can benefit from the information without suffering from information overload (sub c)). This comply and explain approach should only be replaced by a mandatory regime for exceptionally important cryptocurrencies or token-based ventures (sub d)).

a) Preconditions for an Effective Blockchain Governance Code

Before exploring the content of a Blockchain Governance Code, we have to briefly address the conditions for its effectiveness as well as some principled objections. In this domain, three issues stand out: first, sufficient incentives must be in place for cryptocurrencies or token sellers to adopt the Code; this is mainly a question of competitive advantage. Second, to the extent that the Code encourages user participation and empowerment, we must credibly rule out user apathy. Third, it should be considered to what extent such a Code would erect barriers to entry for newcomers.

Starting with the first and most important prerequisite, it is common ground that voluntary governance codes only work if those adopting them gain an advantage vis-à-vis their competitors;[171] otherwise, compliance costs counsel against their adoption. This requires that competition exists at all in the blockchain ecosystem. In oligopolistic markets such as, for example, the market for credit ratings, a governance code has largely failed to deliver behavioral change; the European legislator therefore switched from code-based self-regulation to command-and-control regulation in late 2008.[172]

However, from a competitive perspective, there are reasons to be more optimistic about the effectiveness of a potential Blockchain Governance Code. Competitors exist in sufficient

---

[167] Clarke and Branson (n 137) 4-5, 11; Roberts (n 160) 197; Eberhard Vetter, 'Der Deutsche Corporate Governance Kodex – nur ein Testballon für den Gesetzgeber?' (2004) ZIP 1527.
[168] Grundmann (n 137) § 14 para. 12.
[169] Cf. Janet Yellen, Letter to Congressman Mick Mulvany (September 4, 2015), https://de.scribd.com/document/283714666/Janet-Yellen-Response-to-US-Representative-Mick-Mulvaney-on-Bitcoin, at 8 (stressing the need to balance regulation of cryptocurrencies and incentives for innovation); see also Walch (n 75) 891.
[170] Klaus J. Hopt, 'Comparative corporate governance: the state of the art and international regulation', in: Fleckner/Hopt (eds.), *Comparative Corporate Governance* (Oxford, OUP, 2013), 3, 18.
[171] Cf. Clarke/Branson (n 137) 5; Leyens (n 17) 412.
[172] Niamh Moloney, *EU Securities and Financial Markets Regulation* (OUP, 2014) 644-648; Leyens (n 17).

numbers. Technically, it is possible to start a novel cryptocurrency either via a hard fork[173] or a token sale.[174] Both possibilities are widely used currently. Other than in the case of companies, a hard fork specifically enables developers to copy an existing cryptocurrency and change it only in one, decisive detail.[175] Hence, competitors offering highly substitutable goods or services can arise at any moment in an open-source community like the blockchain ecosystem. This generates specific competitive dynamics and credible threats of rivalry in case of dissent, as the recent Bitcoin hard forks have shown. These competitors are often not negligible fantasy products, but serious contenders: ethereum classic and bitcoin cash, having both arisen of hard forks, currently have the ninth and third highest market capitalization of all cryptocurrencies, respectively.[176] Litecoin, another bitcoin spinoff, occupies the fifth rank.[177]

Low switching costs between these competitors raise competitive pressure on incumbents. Cryptocurrency exchanges enable users to condition from one currency to the other. Rising liquidity in these exchanges makes convertibility ever more feasible;[178] and Bancor provides a decentralized app for inter-currency conversion.[179] Therefore, even though the market capitalization of bitcoin and ethereum is still unrivaled at the moment, competitive pressure is mounting among cryptocurrencies.[180] This holds even more true for ICO-financed decentralized apps that are created almost on a daily basis.

Therefore, offering users a clear framework for governance, and a path to participation, is increasingly viewed as a distinguishing component that confers a competitive advantage. For example, the Tezos token was precisely designed to improve governance matters; ironically, the Tezos foundation has now been caught in a governance crisis of its own.[181] Its staggering success in the token sale, however, arguably testifies to the demand for governance solutions. Furthermore, Ethereum, as the following examples will show (sub b)), already implements a number of desiderata of a governance code. If Ethereum was to endorse large parts of a Blockchain Governance Code, it could prompt competitors to follow suit.

Turning to the second issue, giving more power to users raises concerns of the adequacy of user participation in governance matters. After all, shareholder apathy is often cited as an example for the ineffectiveness of shareholder rights;[182] by analogy, user apathy needs to be confronted by a Blockchain Governance Code. There are at least two answers to this problem. First, mandatory user participation can, and should, be restricted to fundamental matters concerning the blockchain-based organization (below, sub b)5)). This runs in parallel to the largely accepted dogma in corporate law where shareholders equally vote on fundamental matters

---

[173] Nyman and Lindman (n 157).
[174] Hacker/Thomale (n 2); Rohr/Wright (n 2).
[175] Narayanan et al. (n 102) ch 3.6; De Filippi and Loveluck (n 56) 8.
[176] CoinMarketCap, 'Cryptocurrency Market Capitalizations', https://coinmarketcap.com/ (accessed on November 6, 2017).
[177] Id.
[178] Buntinx, 'Cryptocurrency ICO Education – The Basics', (*TheMerkle*, 6 June, 2017), https://themerkle.com/cryptocurrency-ico-education-the-basics/); Rohr/Wright (n 2) 35 ("highly liquid"); eventually, with the increasing number of exchanges (there are 119 currently, see CryptoCoinCharts, 'Cryptocurrency Exchanges / Markets List', https://cryptocoincharts.info/markets/info), liquidity is improving, too: Bajpai, 'Liquidity Of Bitcoins', *Investopedia*, http://www.investopedia.com/articles/investing/112914/liquidity-bitcoins.asp.
[179] Hertzog et al. (n 7).
[180] Hsieh et al. (n 153) 22.
[181] Hochstein (n 11).
[182] Julian Velasco, 'Taking Shareholder Rights Seriously' (2007) 41 *UC Davis L. Rev.* 605, 622.

concerning the company.[183] Second, the online nature of blockchain technology makes user participation more feasible and more expectable; after all, those using the technology often (though not always) do so out of a desire to acquire voice and avoid a system steered by a central authority.[184]

Finally, it could be said that any type of regulation at the end of the day erects barriers to entry that unfairly advantage incumbents over newcomers, and, by extension, lowers competitive pressure. However, this argument has least force in a comply or explain regime where newcomers unilaterally decide what parts of a governance code they would like to implement. Therefore, although the success of a Blockchain Governance Code cannot be guaranteed, its effectiveness is sufficiently plausible to be investigated in detail. If, at the end, a governance code did not lead to significant behavioral change, the uptake rate and explanations for non-adoption still generate knowledge for regulators to base more coercive regulation on.[185] Therefore, the next part sets out possible contents of a Blockchain Governance Code.

b) The Content of a Blockchain Governance Code

The content of a Blockchain Governance Code should be determined by a representative working group that comprises experts and stakeholders as well as user representatives; eventually, this group could evolve into a self-regulatory organization, an "ICANN for blockchains" (below, Part IV.3.). Proposals for the Code's content can only be sketched in this paper; however, the following guidelines can be offered. Overall, the Code should contain provisions on: i) the creation of organs that represent certain stakeholders; ii) transparency, especially of decisions by core developers; iii) fiduciary duties owed by core developers; iv) foundational rules of blockchain-based cryptocurrencies; v) rights of the user community; vi) rules on hard forks; and vii) rules for mining pool operators. Following the example of the UK Corporate Governance Code,[186] *Main Principles* as well as *Specific Rules* should be included in the Blockchain Governance Code; the former provide a general framework of good governance and guide the interpretation of the rules, which in turn spell out the implementation of the principles with greater precision.

1) Establishing Organs: The Group of Core Developers and the Community of Users

The UK Corporate Governance Code starts with the observation that "[e]very company should be headed by an effective board which is collectively responsible for the long-term success of the company."[187] The cryptocurrency ecosystem, by contrast, has been characterized by loose and informal coalitions so far; the lack of formal authority has led to a lack of accountability and foreseeability – to complex behavior at the expense of users (see Part III.). The first major challenge in the elaboration of a good governance scheme is thus the creation of clearly delineated organs whose members have certain rights and duties. This is a necessary precondition for formulating rights that one group of stakeholders has vis-à-vis another. Therefore, the first *Main Principle* of the Blockchain Governance Code ought to be:

---

[183] Velasco (n 182) 623.
[184] See, e.g., Hope et al. (n 6) 6.
[185] Patrick C. Leyens, 'Selbstbindungen an untergesetzliche Verhaltensregeln', (2015) 215 *AcP* 611, 614; Leyens (n 17).
[186] UK CGC (n 132) 4 para. 2.
[187] UK CGC (n 132) Section A.1.

Blockchain-based organizations must establish organs for core developers (responsible for the management of everyday affairs) and users (responsible for deciding fundamental matters).

Borrowing a simple version of a principal-agent model from corporate governance, we may liken owners of cryptocoins to shareholders, i.e., to principals; and core developers to managers, i.e., to agents. This also implies that blockchain-based organizations should primarily cater to the interests of users who invest in them – and not to groups of miners or core developers. Such a perspective embodies the spirit of Nakamoto's Bitcoin White Paper, which introduced blockchain technology as a means to overcome the problem of trusted parties precisely to allow for decentralized but secure interaction between diffused users.[188] However, it does not prevent developers from taking external factors, such as financial stability and the concern of stakeholders other than users, into account, too (see below, 3)).

Specific Rules can govern the formation of the respective organs. While everyone owning a cryptocoin (henceforth the term "user" shall be restricted to these owners[189]) forms part of the community of principals, it is more difficult to clearly establish who should count as a core developer. Therefore, each cryptocurrency (bitcoin, ethereum) should appoint, as a first step, a group of core developers by majority vote of the community of users. In the case of token-based ventures (Filecoin; Status; Bancor, etc.), however, a development team is generally already identified in the white paper; if this is the case, this team should form the initial core developer organ. From then on, new core developers should be appointed by a majority vote of the existing group of core developers.

This departs significantly from corporate governance practices where the influential Cadbury Report, for example, already recommended as a key corporate governance improvement the establishment of a nomination committee with independent directors to propose new board member.[190] However, a nomination committee seems excessively burdensome for the cryptocurrency ecosystem in which many core developers, still, contribute to the project on a voluntary and unpaid basis. One must be careful not to create compliance costs that would deter most cryptocurrencies from applying the Code in the first place. This may be different for profit-driven token-based ventures. However, furthermore, existing developers, in the highly specialized field of blockchain-based organizations, have the expertise to know who might have the requisite skills to fill a new position; independent nomination procedures are therefore best reserved for a time when cryptocurrencies have gained even greater market capitalization, or token-based organizations have entered mainstream business. Vis-à-vis a vote by the user community, appointment by existing members allows for more flexible and faster appointments; however, as a balancing element, users should have a right of veto in the appointment of single new members to the group of core developers.

Finally, it seems unnecessary to create a separate organ for miners: while essential to the functioning of cryptocurrencies, miners are (most often) also users as they receive cryptocoins in compensation for mining. However, their existence points to significant heterogeneity within the pool of users, ranging from owners of small amounts of cryptocoins to highly influential miners. Particularly powerful miners (the operators of so-called mining pools) therefore ought to be subjected to specific rules of conduct (below, 7)).

---

[188] Nakamoto (n 43) 1.
[189] Note that one can own cryptocoins without running a node, see, for bitcoin, Antonopoulos (n 41) 6.
[190] The Committee on the Financial Aspects of Corporate Governance, *Report* (Gee, 1992) para 4.15; Tricker (n 136) 45; see now UK CGC (n 132) Section B.2.

In sum, the two organs of a cryptocurrency or a token-based organization representing the two main stakeholders are: the group of core developers, and the community of users (mirroring the board of directors, and the general meeting of shareholders), with a special, separate regime governing mining pool operators.

2) Transparency

Now that the organs have been formed, specific rights and obligations can be attached to membership of them. A first and pressing requirement is to enhance the transparency of managerial decision making.[191] In corporate governance, this is achieved, inter alia, by board reports. In the words of the UK Corporate Governance Code: "The board should present a fair, balanced and understandable assessment of the company's position and prospects".[192] Transparency also ranks prominently in other corporate governance contexts, for example in financial reporting, risk management, and internal control mechanisms.[193] We can therefore formulate a second *Main Principle*:

The decision-making process of core developers should be transparent to users, particularly in matters pertaining to the update of the protocol.

The *Specific Rules* should include the following: first, the group of core developers is obliged to maintain a list of current core developers that has to be published on a universally accessible website. Second, in corporate law, shareholders have a right to inspect books and records, which is perceived as a disciplining tool contributing to good corporate governance.[194] Similarly, users should have a right to demand information from core developers about past or present decisions that might affect the valuation of cryptocoins or the rules governing transactions. Finally, core developers ought to report annually on the reasons for making updates to the protocols, and on the extent to which miners have been involved in managerial decisions (see also below, 7)). Ethereum is already publishing transcripts of core developer calls, showing that transparency is not prohibitively burdensome.[195]

3) Fiduciary Duties

Fiduciary duties are another staple of corporate law owed by management.[196] Similarly, scholars have recently proposed that fiduciary duties should play a greater role in the regulation of data-driven environments. Jack Balkin has argued that data processing companies should be considered information fiduciaries vis-à-vis their clients, implying duties of loyalty and care.[197] In a similar vein, Angela Walch has contended that blockchain core developers and significant

---

[191] Gervais et al. (n 56) 59.
[192] UK CGC (n 132) Section C.1.
[193] UK CGC (n 132) Section C.3.
[194] See, e.g., Lawrence A Hamermesh, 'Twenty Years after Smith v. Van Gorkom: An Essay on the Limits of Civil Liability of Corporate Directors and the Role of Shareholder Inspection Rights' (2006) 45 Washburn LJ 283; Stephen A Radin, 'The New Stage of Corporate Governance: Section 220 Demands' (2005) 26 Cardozo L. Rev. 1595; Randall S Thomas, 'Improving Shareholder Monitoring of Corporate Management by Expanding Statutory Access to Information' (1996) 38 Ariz. L. Rev. 331.
[195] Tapscott and Tapscott (n 113), 15.
[196] Tricker (n 142) 102-103.
[197] Jack Balkin, 'Information Fiduciaries and the First Amendment' (2016) 49 UC Davis Law Review 1183; id., 'The Three Laws of Robotics in the Age of Big Data' Ohio State Law Journal (forthcoming), https://ssrn.com/abstract=2890965, 12-15.

miners should assume fiduciary duties towards users who (impliedly) entrust them with the power of maintaining the code and updating the chain.[198] Moreover, if some types of blockchain-based organizations are regarded as partnerships in a legal sense,[199] fiduciary duties may arise by default as a matter of company law.

This section discusses the fiduciary duties of core developers (section vii develops rules for miners). Importantly, in corporate law, fiduciary duties are part of general corporate law[200] and are (generally) mandatory in nature;[201] hence, they are not part of the Corporate Governance Code. Nevertheless, I would like to submit that, in order to balance incentives for experimentation with accountability, fiduciary duties should in general be included in the Blockchain Governance Code, and thus subjected to the comply or explain framework. Only for particularly important blockchain-based organizations should they be made mandatory (see below, Part IV.3.).

In corporate law, the main question is to whom these duties are owed to: only to shareholders; to all stakeholders; or even to the public at large and to the environment?[202] Similarly, we may ask whether core developers should owe fiduciary duties of loyalty and care to the community of users only; also to other stakeholders, such as exchanges, wallet designers and employees; or whether they should even assume responsibility for, and act in the interest of, financial systemic stability.

In comparative corporate governance, the so-called enlightened shareholder value approach has lately gained prominence.[203] It posits that the interest of shareholders should be at the center of the actions of management, but that the interests of other stakeholders and the public at large can also be taken into account. The main argument for not strictly equating shareholder with stakeholder interests is that stakeholders typically maintain contractual relationships with the company that they can use to protect their interests.[204] Similarly, one may argue that cryptocurrency stakeholders (e.g. mining pool operators; exchanges; wallet providers) are powerful, centralizing intermediaries[205] who may, in contrast to users, contractually safeguard their interests. Nevertheless, questions of financial systemic stability should become

[198] Angela Walch, 'Call Blockchain Developers What They Are: Fiduciaries', American Banker (August 10, 2016); for a detailed discussion, see id. (n 72), particularly Part II (applying Tamar Frankel's definition of fiduciaries); cf. also De Filippi and Loveluck (n 56) 10 ("a small group of developers and software engineers who have been *entrusted* with key roles for the development of this technology") [italics in the original quote].
[199] See above (n 151), and below (n 201).
[200] Hopt (n 170) 55.
[201] Mads Adenas and Frank Woolridge, *European Comparative Company Law* (CUP 2009) 271-275; under Delaware law, fiduciary duties are mere default rules, however, for LLCs and LPs; see, generally, Mohsen Manesh, 'What Is the Practical Importance of Default Rules Under Delaware LLC and LP Law?' (2012) Harvard Bus L Rev Online 121.
[202] See, e.g., Jonathan R Macey, 'An economic analysis of the various rationales for making shareholders the exclusive beneficiaries of corporate fiduciary duties' (1991) 21 Stetson L. Rev. 23.
[203] Grundmann (n 137) § 14 para. 20; Paul Davies, Enlightened shareholder value and the new responsibilities of directors, WE Hearn Lecture at the University of Melbourne Law School (2005), http://law.unimelb.edu.au/__data/assets/pdf_file/0014/1710014/94-Enlightened_Shareholder_Value_and_the_New_Responsibilities_of_Directors1.pdf; Simon Deakin, 'The Juridical Nature of the Firm' in Thomas Clarke and Douglas Branson (eds) *The SAGE Handbook of Corporate Governance* (SAGE 2012) 113, 117-118, 132; Clarke and Branson (n 137) 3; Tricker (n 136) 58.
[204] Grundmann (n 137) § 14 para. 22.
[205] Gervais et al. (n 56) 55-56.

increasingly important to managerial decision making as the market capitalization of a cryptocurrency rises. The center of fiduciary duties, however, should be users who, other than most stakeholders, are not in a position to individually negotiate with the management to safeguard their interests.

Continuing this line of reasoning, a third *Main Principle* should be:

Core developers owe fiduciary duties to users.

Specific Rules should include the following:[206] first, core developers owe a duty of loyalty to users; they have to act in their best interests. However, this does not prevent them from taking the interests of other stakeholders, and the financial system at large, into account in their decision making, provided they make these considerations transparent. Second, core developers owe a duty of care to users: they have to act competently and use adequate, state-of-the-art technical means to assure the smooth functioning of the blockchain, for payments (in the case of cryptocurrencies) or (additionally) for the product they are developing (storage app, messenger platform etc.). However, in order to shield them against overwhelming damage claims by users, individual liability caps need to be installed (at least for cases of negligent violation of fiduciary duties) that make insurance against liability risks affordable. This significantly mitigates the disincentivizing effect of liability for assuming responsibility as a core developer in the first place.

4) Adherence to Foundational Blockchain Rules

In corporate law, the duty of good faith prevents managers from violating generally accepted basic corporate norms.[207] Similarly, the group of core developers should promise to adhere to the foundational rules of blockchain-based organizations. Particularly, this implies the fourth *Main Principle*:

The blockchain-based organization adheres to the following two basic rules. First, in case of conflicting chains coming into existence, the longer chain is regarded as the authentic one. Second, the information contained in the authentic chain cannot be retrospectively changed.

As was shown, both basic rules were violated in the Bitcoin and the Ethereum hard fork, respectively. The first rule is crucial because it enshrines user sovereignty over the authenticity of the chain; such a decentralized consensus thus empowers users. The second rule prevents circumvention of the first one, and adds a decisive element of stability to validated transactions on the chain. Because both rules, eventually, flow from user power, exemptions from these rules ought to be treated as a matter of competence of the user community – to which we now turn.

5) Community Vote on Fundamental Matters

The competence of the general assembly of shareholders to vote on fundamental matters pertaining to the company is a key component of internal governance by voice.[208] Analogously, the fifth *Main Principle* ought to be:

---

[206] See Walch (n 72) 19.
[207] Melvin A Eisenberg, 'The duty of good faith in corporate law' (2006) 31 Del. J. Corp. L. 1, 24.
[208] Velasco (n 143) 610-614.

The community of users should have the right to vote on fundamental matters concerning the blockchain-based organization.

This is a desideratum that is also voiced by the cryptocurrency community.[209] In fact, returning power to users corresponds precisely to the ethos of blockchain's founding document.[210] Fundamental matters are indeed best decided by all those directly concerned, i.e., the users; to prevent a deadlock, however, a majority vote must suffice for proposals to be adopted.[211] After this, miners also, inevitably, need to back the new implementation to ensure the proposal succeeds in reality. While this has always been a requirement,[212] the additional user vote would increase transparency and voice in otherwise opaque updating procedures concerning fundamental matters.

Specific Rules may list examples of fundamental matters: first, exceptions to the above-mentioned foundational rules should only be permissible if the majority of users approve of them. As mentioned, Ethereum surveyed users, asking them to express their opinion about the hard fork violating the second foundational rule (no rewriting of the chain) before its implementation; the majority of participants had approved it.[213] Second, hard forks pushed by the group of core developers should be subject to user approval.[214] Third, the question of whether a blockchain-based organization ought to comply with the Blockchain Governance Code should also be decided by the user community – after all, the Code seeks to improve governance first and foremost in the interest of users.[215] As an exception, arguably, the non-adoption of parts of the Code may be decided by the group of core developers in utility or investment tokens if specific sections of the Code would render their projects impossible or highly unlikely to succeed.

Procedurally, two ways of weighting user votes are possible: either, one user (more precisely one account) gets one vote; or votes are weighted by the financial stake that users have in the respective system, i.e., by the amount of cryptocoins owned. As is well-known, voting by shareholders follows the second alternative: voting power follows share size.[216] This prevents disproportional influence of those only marginally affected by a decision (empty voting). A similar reasoning could be applied to cryptocurrencies; as seen, Ethereum has established a voting procedure that was used for the 2016 hard fork, and is now used again for further hard fork proposals (carbonvote). In this voting mechanism, votes are weighted by the amounts of ethers owned.[217]

---

[209] Cf. the proposals to reinforce user voice in Bitcoin Core, De Filippi and Loveluck (n 56) 9; see also Pete Rizzo, 'Bitcoin Unlimited: Mining Power Should Determine Hard Fork' (*CoinDesk*, March 29, 2017), http://www.coindesk.com/bitcoin-unlimited-mining-power-should-determine-hard-fork-outcome; and https://github.com/bitcoin/bips/blob/master/README.mediawiki.

[210] Nakamoto (n 43) 1.

[211] Note that this would not require all users to run a node, which would be highly impractical (see Valery Vavilov, 'Keep Calm and Bitcoin On' (*Medium*, January 18, 2016), https://medium.com/@BitFuryGroup/keep-calm-and-bitcoin-on-4f29d581276 under 'Mass Rule is Not Appropriate for Bitcoin'; rather, an off-chain polling system would need to be installed, see below (n 220).

[212] See above (n 98).

[213] See above (n 96).

[214] This would leave the right of ordinary users to create spin-off versions of existing cryptocurrencies untouched; see above, Part IV.1.b), and below, Part IV.2.a)6).

[215] By contrast, in corporate governance, it is the board that takes comply-or-explain decisions, see Hopt (n 170) 23.

[216] Tricker (n 142) 86.

[217] See carbonvote.com, under Carbonvote.com Mechanism 2) (accessed June 9, 2017).

However, two reasons speak decisively for the first alternative of one account, one vote. First, it would prevent collusion between mining pool operators (who typically own significant amounts of cryptocoins due to their mining activities) and core developers. This was identified as one of the key imperfections of current governance mechanisms. Second, it corresponds to the more egalitarian background of open source communities vis-à-vis for-profit companies; specifically, in permissionless blockchain environments like Bitcoin, the generally equal capacity of nodes to contribute to the chain speaks in favor of equal voting rights for all users.[218] A remaining concern is that a single user may have multiple accounts, enabling her to illicitly cast several votes. However, one would likely have to amass a prohibitively high number of such identities to make a difference in a vote;[219] most likely, the resulting voting pattern would be much closer to user equality under a one account, one vote rule than under a financial weighting rule, where "multiple voting" would be the default case as a consequence of crypto wealth inequality.

These voting rules collectively guarantee that whenever the financial stake or the participation of users in the respective cryptocurrency is fundamentally affected, they cannot be overruled by collusion between core developers, potentially in conjunction with mining pool operators. Core developers, finally, would be under an obligation to set up the necessary technical infrastructure that allows for communication between users and for conducting voting procedures. Carbonvote shows that voting coupled to accounts is technically possible in a cost-effective way.[220] Regarding communication, in Bitcoin, core developers until recently had the capacity to send messages to all users, adding to the unequal distribution of power within the network.[221] To avoid spamming and security threats, this privilege should not be conferred on all users; however, users may select a group of user representatives that has the right to send messages to all users. This could provide a crucial counterbalance to the informal alliances between core developers and/or mining pool operators, allowing for constructive coordination of user interests before user votes. Carbonvote, for example, was accused of being "diligently hidden" and framed "pro-fork" ahead of the user vote on the Ethereum hard fork.[222]

6) Rules on Hard Forks

"The right to fork code is built into the very definition of what it means to be an open source program."[223] Nevertheless, as the case studies have shown, hard forks are another primary source of instability in cryptocurrency environments and can be identified as tipping points that, in the case studies, marked the transition from a stable to an unstable state of the system. Therefore, the Code should contain a sixth *Main Principle* on hard forks:

Rules governing hard forks must balance the users' right to exit with the interest of remaining users in the continued stability of the blockchain-based organization.

---

[218] Cf. on the equality of nodes Liao (n 44); Antonopoulos (n 41) 111.

[219] Voting could be subjected to a minimum of cryptocoins owned by the account, further raising the costs of multiple voting; this is implemented by carbonvote.com, see there under Carbonvote.com Mechanism 3) (accessed June 9, 2017).

[220] However, utmost transparency must be observed in communicating the possibility, and the exact ways, of voting to prevent steering efforts by core developers, see above (n 95).

[221] Antonopoulos (n 41) 157; Walch (n 75) 845; Gervais et al. (n 56) 57; however, this function has now been deactivated for fear of abuse: https://bitcoin.org/en/alert/2016-11-01-alert-retirement.

[222] Parker (n 90).

[223] Nyman and Lindman (n 157) 8.

By virtue of *Specific Rules*, those initiating a hard fork (users or developers) should be under an obligation to implement suitable measures to stabilize the value of existing coins, and to cooperate fully with all stakeholders (including wallet designers and exchanges) to guarantee a smooth transition into the newly created chain. They should also be required to install features that prevent unnecessary conflict between the old and the new chain, for example replay protection schemes.[224] While bitcoin cash offered such protection, the SegWit2x hard fork proposal lacked it, which significantly increased uncertainty for those willing to stay on the legacy chain before the proposed fork.[225] Finally, as seen, hard forks initiated by core developers should be subjected to user approval.[226]

7) Rules for Mining Pool Operators

In the current state of large cryptocurrency systems like bitcoin, individual miners (called solo miners) are very unlikely to muster enough computing power to successfully mine a block and to receive cryptocoins in reward.[227] Therefore, like players teaming up to collectively win a lottery and distribute the reward, solo miners usually join mining pools.[228] These are managed, on a technological level, by pool-mining protocols that coordinate the contributions of hundreds or even thousands of miners.[229]

Mining pools are (mostly) run by so-called mining pool operators.[230] These operators de facto wield large amounts of computing power – including the ability to direct these resources in support of specific chains in case there is a fork.[231] As it were, they bundle and exercise the "voting rights" of individual miners, without the explicit authority to do so. In the summer of 2017, almost 95 % of Bitcoin and almost 80 % of Ethereum mining power was controlled by 10 and 6 mining pools, respectively.[232]

Therefore, mining pool operators occupy a middle ground between core developers and individual users. They do not directly form part of the management team, as they are not implementing updates to the code. However, they exert informal power and control through their miners' computing power. There is a growing concern that the use of that power may be diametrically opposed, at times, to the preferences of the user community.[233]

---

[224] Replay protection prevents an attacker to conduct the same transaction twice, once on the old and once on the new chain, after a chain split, see JP Buntinx, 'What is a Bitcoin Replay Attack?' (*TheMerkle*, March 22, 2017).
[225] Deschapel (n 105), under "Unprecedented circumstance"; Aaron van Wirdum, 'SegWit2X and the Case for Strong Replay Protection (And Why It's Controversial)' (*Bitcoin Magazine*, September 22, 2017), https://bitcoinmagazine.com/articles/segwit2x-and-case-strong-replay-protection-and-why-its-controversial/https://www.coindesk.com/opinion-segwit2x-doomed-fail/.
[226] See above, Part IV.2.a)5).
[227] Antonopoulos (n 41) 207; Narayanan et al. (n 102) ch 5.2.; this was one of the reasons for the bitcoin gold fork.
[228] Gervais et al. (n 56) 56; Bonneau et al. (n 45) 108.
[229] Antonopoulos (n 41) 207-208.
[230] Antonopoulos (n 41) 209; the alternative framework, P2P pools (see, e.g., http://p2pool.org/), do not give rise to the discussed governance issues as they lack a central operator that may intentionally direct the mining power of the miners, cf. ibid 209-210.
[231] Gervais et al. (n 56) 57.
[232] Loi Luu et al., 'SMARTPOOL: Practical Decentralized Pooled Mining' USENIX Security Symposium 2017, people.cs.uchicago.edu/~teutsch/papers/smartpool.pdf.
[233] Rizzo (n 209); JP Buntinx, 'Jihan Wu Wants To Accelerate The Bitcoin Unlimited Hard Fork Regardless of Community Sentiment' (*News BTC*, March 19, 2017),

Hence, the seventh *Main Principle* ought to postulate:

Mining pool operators must refrain from covertly influencing core developers and must direct mining power responsibly.

Specific Rules of transparency should apply to them for the adoption of, or other types of support for, new versions of reference implementations, particularly after a hard fork. This should prevent covert collusion between mining pool operators and core developers. Irresponsible use, in turn, arises primarily from the intentional exploitation of mining power for inappropriate ends. Thus, first, mining pool operators should be barred from supporting proposals or updates that violate the foundational rules of blockchain unless these violations have been approved by community vote. Second, they would have to provide detailed reasons for refusing to back an update that was approved by the community of users.[234] Finally, the use of disproportionate computing power to launch a so-called 51% attack, exploiting a specific vulnerability in the blockchain set up,[235] would count as irresponsible. Whenever mining pool operators control more than 50% of total computing power in a network, they could theoretically launch such an attack. Arguably, this would undermine trust in the entire network and rapidly devalue the currency.[236] As concerns rise about the possibility of a 51% attack,[237] a duty of responsible use legally binds mining pool operators that, until now, have been bound by their goodwill alone.

The thorniest question is whether miners should additionally be subjected to fiduciary duties.[238] This would imply, for example, a duty of care, i.e. of competent action, not implied by the duty of responsible use. Arguably, however, fiduciary duties of loyalty and care for core developers ought to be sufficient (above, 3)) if they are paired, as foreseen, with: a) transparency obligations of core developers towards users concerning the influence of mining pool operators (above, 2)); and b) the accountability rules for miners just discussed. Core developers are thus bound to resist the undue influence of mining pool operators in order to avoid breaching their fiduciary duties; and disclosure obligations bring these attempts to the attention of the public. Therefore, fiduciary duties for mining pool operators seem unnecessary. Avoiding them, while holding operators accountable according to the seventh *Main Principle*, could mitigate power imbalances without deterring current or future mining pool operators from assuming these functions in the first place.

c) Comply or Explain: Cognitively Optimized Disclosure

The second step in a comply and explain regime is to ensure that information about the content of the Blockchain Governance Code, and about the decision of the individual cryptocurrency about whether to comply or not, is adequately designed so that it can be expected to be

---

http://www.newsbtc.com/2017/03/19/jihan-wu-wants-accelerate-bitcoin-unlimited-hard-fork-regardless-community-sentiment/.

234 See above (n 212) and accompanying text.

235 Antonopoulos (n 41) 211-213; for other vulnerabilities, see, e.g., Maria Apostolaki et al., 'Hijacking Bitcoin: Routing Attacks on Cryptocurrencies' IEEE Security and Privacy (forthcoming), https://arxiv.org/abs/1605.07524.

236 Jonas Borchgrevink, 'Warning: Ghash.Io Is Nearing 51% – Leave the Pool' (Cryptocoins, 09/01/2014), https://www.cryptocoinsnews.com/warning-ghash-io-nearing-51-leave-pool/.

237 Luu (n 232) 2; Borchgrevink (n 236); descarte, 'Dwarfpool is now 50.5%' (Ethereum Community Forum, March, 2016), https://forum.ethereum.org/discussion/5244/dwarfpool-is-now-50-5.

238 See Angela Walch, 'Call Blockchain Developers What They Are: Fiduciaries', American Banker (August 10, 2016); id. (n 72) (presenting arguments for fiduciary duties of "significant miners").

understood by the prospective recipients.[239] Blockchain-based organizations can make comply or explain decisions at the level of each individual provision of the Code; hence, they can comply with the entire Code, with the exception of the rules on fiduciary duties, for example.

Disclosure of these decisions should help potential and current users make informed decisions about what cryptocurrency to use; by influencing user choice, it should have a disciplining impact on core developers as well. This, however, invites a host of problems that have recently been discussed as limits to the disclosure paradigm in private law. Simply put, research in behavioral economics suggests that people are often not motivated to read standardized information, are easily overwhelmed by an excess of information, and tend to process information in a biased way.[240]

Therefore, it must be expected that most users will not take the time and effort to actually read and cognitively digest a Blockchain Governance Code, or lengthy disclosures regarding compliance with it. Rather, one must design a simple signaling mechanism that conveys salient and highly condensed information about whether a cryptocurrency complies with the Code or chooses to deviate from it. For this, one might use what I have called, in recent contributions, cognitively optimized disclosure.[241] This consists of information put in simple, plain language, which also conveys the information in different layers of increasing complexity. Thereby, the cognitive and motivational heterogeneity of users is actively addressed.

Before first accessing a web client or downloading software enabling them to trade in a certain cryptocurrency or to participate in an ICO, users would see a message about whether the blockchain-based organization complies with the Code. Differences ought to be signaled by the background color of the message, e.g., green for compliance, yellow for partial compliance, and red for non-compliance.

The hyperlinked second layer of information that users can access would contain a link to a PDF version of the Code and, in the case of non-compliance, a statement explaining why the organization has opted out of the Code, or a particular provision, and what alternative measures, if any, have been implemented to ensure good governance.[242] Furthermore, it ought to contain a link to a website that lists all (relevant) tokens and their respective compliance decisions, again coded in color.[243] This list would allow users to compare and choose blockchain organizations based on their governance commitments.

Such a setup both limits the burden on the developers for signaling compliance or non-compliance, and it increases, by virtue of its simplicity and salience, the chances of reaching a significant part of the user base. Organizations that opt out of the governance code should, however, be required to revisit their decision annually and, if they continue to opt out, explain why the Code continues not to fit their needs.

---

[239] See generally on the importance of understandable disclosure Philipp Hacker, 'Nudge 2.0: The Future of Behavioural Law and Economics, in Europe and Beyond' (2016) 24 ERPL 297, 313; id, *Verhaltensökonomik und Normativität* (Mohr Siebeck 2017), Parts III and IV; for corporate governance explanations specifically, see Art. 8-10 of Commission Recommendation 2014/208/EU of 9 April 2014 on the quality of corporate governance reporting ('comply or explain'), OJ 2014 L 109/43.

[240] Ibid.; Omri Ben-Shahar and Carl E. Schneider, *More than You Wanted to Know* (Princeton UP 2014).

[241] See above (n 239).

[242] Cf. Art 46a Annual Accounts Amendment Directive.

[243] The website could be maintained by a financial authority of one state in which cryptocurrencies are particularly active, for example by the US Federal Reserve, or, preferably, by an "ICANN for blockchains"; see below, Part IV.3.

d) From Comply and Explain to Mandatory Compliance

One final lesson can be drawn from corporate governance: for those companies wishing to be listed on stock exchanges, the choice between comply and explain was sometimes replaced by mandatory compliance with the Corporate Governance Code (through the listing rules of the respective stock exchanges).[244] The idea is that those companies whose shares are particularly frequently and publicly traded should adhere to the minimal requirements formulated by the applicable Corporate Governance Code.

Similarly, those individual cryptocurrencies or token-based ventures that assume a certain weight in the financial system should be forced to comply with the Blockchain Governance Code. Arguably, this could be the case once a certain cryptocurrency is granted legal tender status, or once a certain threshold of market capitalization is passed. In a similar vein, Angela Walch has argued that, once cryptocurrencies become large enough to be considered "financial market infrastructure", they should be subject to financial stability rules of the international financial market architecture, for example the Principles for Financial Market Infrastructures.[245] Corporate governance mechanisms ought to be another building block in this regime. The threshold separating the comply and explain from a mandatory regime would spare small cryptocurrencies and token-projects that tend to be more experimental in their set-up. However, it would implement necessary stability rules once the cryptocurrency, or token-based venture, becomes a more serious building block in the financial system.

3. The Future of Blockchain Governance: ICANN and Beyond

The rise of the Internet has shown how a decentralized structure lacking governance mechanisms can be gradually transformed and subjected to self-regulation by an organization that brings together various stakeholders: the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN arose from the necessity to coordinate information flows across initially separate networks and, more specifically, to assign addresses in the global domain name space.[246] Similarly, an "ICANN for blockchains" may eventually be necessary to the extent that permissionless blockchains, and the cryptocurrencies and token-based ventures they give rise to, become more interconnected;[247] their respective coins convertible through exchanges;[248] and governance problems replicate in similar fashion within different blockchain-based organizations.[249] This novel institution would have four main tasks. First, drawing on diverse stakeholder input, it would develop and update the Blockchain Governance Code. Second, it would oversee the implementation of, and compliance with, this Code; this includes providing information to users about the respective degree of compliance of each blockchain-based organization.[250] Third, it would seek to monitor the stability, and systemic risk, of the respective cryptocurrencies as well as their interconnectedness with one another and with the remaining financial system. In this, it could draw on the complexity analyses suggested

---

[244] Hopt (n 162) 11; Grundmann (n 137) § 14 para. 8.
[245] Walch (n 75) 854.
[246] Jonathan Weinberg, 'ICANN and the Problem of Legitimacy' (2000) 50 Duke Law Journal 187, 189-191.
[247] Cf. Tapscott and Tapscott (n 113), 17.
[248] See CryptoCoinCharts, 'Cryptocurrency Exchanges / Markets List', https://cryptocoincharts.info/markets/info, listing 119 exchanges; Bajpai, 'A Look At The Most Popular Bitcoin Exchanges', *Investopedia*, http://www.investopedia.com/articles/investing/111914/look-most-popular-bitcoin-exchanges.asp.
[249] Cf. also Tapscott and Tapscott (n 113), 33.
[250] See above, Part IV.2.b).

above, [251] and address frictions arising from the parallel and interconnected nature of cryptocurrencies.[252] Fourth, to bypass the intricacies of international private law as applied to blockchain-based organizations,[253] it could even act as a dispute resolution organization for matters concerning blockchain governance.

ICANN is well-known to be criticized often for unfairness, illegitimacy and misrepresentation of stakeholders.[254] A corresponding institution for blockchain-based organizations would have to attempt to avoid these pitfalls while preserving a meaningful mechanism of decision making; this opens one important avenue for future research of blockchain governance that can build on empirical and theoretical scholarship concerning ICANN. Moreover, the seven *Main Principles* and subordinate rules just expounded also await further analysis of their potential costs and benefits, as well as optimal enforcement rules. These questions frame an intriguing research agenda, but transcend the scope of this paper.

What can be said, however, is that the Blockchain Governance Code should be viewed as a dynamic instrument: it ought to start with a simple version, to which one may add provisions as novel problems become apparent. In fact, Corporate Governance Codes also developed precisely in such an incremental way.[255] Their rules have, however, grown substantially over the years, a development that is increasingly viewed critically in the literature.[256]

Therefore, Blockchain Governance Codes should refrain both from regulatory excesses and from an overreliance on disclosure. In a first draft, not all of the problems that have arisen in corporate governance over the years need to or should be addressed. The law of blockchain-based organizations is a relatively young field that will benefit from an attempt to limit the number of legal provisions to those necessary to solve the most pressing of its current problems; otherwise, compliance costs will likely deter not only organizations from applying the Code, but will also impede experimentation and socially beneficial innovation in the long run. A Blockchain Governance Code is an attempt to mitigate governance problems by means of soft law, applicable only if organizations voluntarily decide to adopt it, or if they surpass a threshold of financial importance. If, eventually, these strategies prove incapable of providing stability and user protection, nothing prevents regulators from introducing mandatory solutions later. In fact, in a number of areas such as say on pay, insider trading, takeover and rating agency regulation, comply or explain approaches have been gradually replaced by mandatory regulation.[257] However, until we reach this point, it seems prudent first to introduce a comply or explain approach that gives greater leeway to the agents in the system to experiment, and to adapt principles and rules to their specific needs.

---

[251] See above, Part III.3.
[252] See, e.g., the replay protection problem mentioned above (n 224 and text).
[253] See above, Part IV.1.a).
[254] Jonathan GS Koppell, 'Pathologies of Accountability: ICANN and the Challenge of "Multiple Accountabilities Disorder"' (2005) 65 Public Administration Review 94; Michael Geist, 'Fair.com? An Examination of the Allegations of Systemic Unfairness in the ICANN UDRP', (2002) 27 Brooklyn Journal of International Law 903; Weinberg (n 246).
[255] Tricker (n 136) 45-47; 50-52.
[256] See, e.g., Tricker (n 136) 47; Turnbull (n 145); cf. also Thomas Clarke, 'Cycles of Crisis and Regulation: the enduring agency and stewardship problems of corporate governance' (2004) 12 Corporate Governance: An International Review 153.
[257] Leyens (n 17).

V. Conclusion

Recent scholarship has discussed the opportunities, but increasingly also the limits, of blockchain-based architectures such as cryptocurrencies or token-based ventures for serving as a novel backbone of our financial system. The present article adds to this critical perspective by highlighting the instability and unpredictability that has so far proven to be inherent in major blockchain-based organizations such as bitcoin and ethereum. Importantly, it identifies imperfections in existing governance structures as a key source of violations of core blockchain rules that make predictions of the development of these systems highly uncertain.

This article therefore highlights the need to analyze, and optimize, decision-making frameworks in blockchain-based organizations. More specifically, it aims to make two novel contributions to the emerging discussion of the law of blockchain. First, it argues that it is analytically profitable to analyze blockchain-based organizations, in their existing format, as complex systems that exhibit both patterns of regularity and unpredictability. Second, regulators should use rules specifically designed to reduce uncertainty by strengthening the elements of order and regularity in a complex system. Based on the analysis of imperfect governance regimes, this article suggests adapting the theory and practice of Corporate Governance Codes – and their concomitant "comply or explain approach" – to the reality of blockchain-based organizations. In this, it proposes concrete measures to improve the external and internal governance in an attempt to strike a fair balance of power between different stakeholders. Arguably, this would strengthen elements of regularity and order in complex blockchain-based organizations, while allowing developers the discretion to experiment to the benefit of users and the financial system alike.