

THE INDIAN JOURNAL OF LAW AND TECHNOLOGY

Volume 11, 2015

ON MONOPOLISTIC PRACTICES IN BITCOIN: A CODED SOLUTION

Sanya Samtani, Varun Baliga*

This article was the winning entry of the IJLT-SFLC Essay Competition, 2014.

ABSTRACT

The underlying values inherent in the creation of bitcoins are those of decentralization and accessibility. The horizontal power structure is an integral part of bitcoins' architecture – this paper seeks to find a feasible alternative to status quo in order to preserve these characteristics. First, we look at the harms of monopolies and how the concentration of bitcoins is exceptionally harmful to its continued existence. Second, we expose the inadequacies of the existing regulatory frameworks, and discuss how status quo militates against the foundational ideology of bitcoin as a non-institutional cryptocurrency. Third, we undertake a comparative study of the existing regulatory regimes to identify legal and regulatory issues surrounding bitcoins. Finally, we propose a solution to the concern of centralization by discussing the relationship between law, code and the market, and discussing existing coded solutions that may be further improved upon to prevent such monopoly.

Before the advent of pervasive state regulation, the intrinsic value of currencies was driven by scarcity. Money was thus made of animal bones, skins or precious metals.¹ In the contemporary era, its value is derived from the government and its narrative of stability, rule of law and legitimacy. The shortcomings of this trust-based model was the rationale for Satoshi Nakamoto's cryptocurrency, allowing reversible transactions across a communications channel *sans* a trusted third party

* Sanya Samtani is a BCL candidate at the University of Oxford and Varun Baliga is a V Year student at NALSAR University of Law.

1 Joshua J. Doguet, *The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System*, 73 LOUISIANA LAW REVIEW 1119, 1120 (2013).

institution.² Not only did he find the current model cost and time inefficient, but also entailed vesting government regulators with excessive powers – that in the recent past, have been deeply politicized. Bitcoins, instead, would be based on cryptographic proof.³ Double spending would be prevented by a public block chain, i.e., the transactional history of the currency that was earlier entrusted solely with the government mint.⁴ Decentralization, a fiercely horizontal power structure and a robust code, is what drives the world’s first currency entirely outside state control.

The architecture of the bitcoin system merits regulation because, as we argue, it is especially susceptible to monopolization, particularly by mining pools. Some argue that the public block chain and constant vigilance maintained by the bitcoin community represent an improvement from the “trust-based model” of reliance on banks and financial intermediaries – trusted third parties.⁵ The argument goes that the reduced costs and privacy of the architecture of bitcoin offers outweighs the purported benefits of state regulation.⁶ Mining pools are entities that are made up of shared resources of different users who then equally split the reward from such mining based on the amount of work they have put in.⁷ Recent instances of GHash, a mining pool, hovering around the 45% range witnessed sharp criticism for coming close to the 50% threshold. The counter-argument runs that once any single entity exercises control over more than 50%, it has the power to legitimize suspect, and has irreversible,⁸ transactions powers that subvert bitcoin’s decentralized functioning.⁹ The fear of centralization triggered a concomitant fall

2 Satoshi Nakamoto, *Bitcoin : A Peer to Peer Electronic Cash System*, <https://bitcoin.org/bitcoin.pdf> (Last visited June 19,2014.)

3 *Ibid*, at 2-3.

4 *Blockchain*, at <https://blockchain.info/> (Last visited June 19, 2014).

5 Joshua, *supra* note 1, at 1123-1126.

6 Kevin V. Tu and Michael W. Meredith, *Rethinking Virtual Currency in the Bitcoin Age*, 90 WASHINGTON LAW REVIEW 271, 279-282 (2015).

7 *Bitcoin mining pools : What is Bitcoin Mining*, at <http://www.bitcoinmining.com/bitcoin-mining-pools/> (Last visited March 16, 2015).

8 Anita Ramasastry, *Should Mt. Gox be Bailed Out?*, JUSTIA.COM (March 11, 2014) <https://verdict.justia.com/2014/03/11/mt-gox-bailed> [Last visited on July 21, 2015].

9 Anita Ramasastry, *Bitcoin: If You Can't Ban It Should You Regulate It? The Merits of Legalization*, JUSTIA.COM (February, 2014), <https://verdict.justia.com/2014/02/25/bitcoin-cant-ban-regulate> [Last visited on July 19, 2015].

in the value of bitcoin and selling by some of the currency's developers, like Peter Todd.¹⁰ This fear of a single mining pool reaching 51% is well-founded. A group of determined miners can block the entire system with their numbers, apart from engaging in double spending, manipulation of the block chain and devaluation, all of which would be legitimized by the networks controlled by this mining pool. The strength of bitcoin lies in its distributed network – but with the unanticipated prominence of mining pools, networks are steadily coming under the control of single entities.¹¹ Therefore, while 51% is a grave threshold, the aggregation of these networks represents the more egregious, existential threat to the bitcoin community.

Nonetheless, mining pools are greatly advantageous. They enhance computing power; consequently the ability to mine more bitcoins. This incentivizes more miners to join since greater profits are shared equally within the group. Concomitantly, the group gains control of more networks.¹² Now, mainstream *fiat* currencies rely on a central authority to prevent fraudulent transactions. The bitcoin community depends on itself, premised on the independence and vigilance of miners. Therefore, the public updated block chain identifies fraud, such as the use of spent bitcoins (double spending) or fake bitcoins. However, it ignores the possibility of mining pools working in sync. Therefore, today an overwhelming majority of bitcoins are not controlled by independent miners but by pools.¹³ This steady centralization is ironic, since the idea behind cryptocurrencies was to escape from it. Further, it also has pernicious consequences for the relationship of trust that it shares both within the community and with the economy. The future of bitcoins, its valuation and use all depend on the level of trust. Governments enjoy a presumption of trust but bitcoins' trust is grounded in the miners, and

10 Peter Todd, *Why I just sold 50 of my bitcoins*, June 13, 2014 http://www.reddit.com/r/Bitcoin/comments/281ftd/why_i_just_sold_50_of_my_bitcoins_ghashio/ ([Last visited June 19, 2015].

11 Dan Goodin, *Bitcoin Security Guarantee Shattered by Anonymous Miner with 51% Network Power*, <http://arstechnica.com/security/2014/06/bitcoin-security-guarantee-shattered-by-anonymous-miner-with-51-network-power/> [Last visited June 19, 2015].

12 *Mining Pools v. Solo Mining*, *Devtope*, http://www.devtope.com/doku.php?id=mining_pools_vs_solo_mining [Last visited June 19, 2015].

13 Michael McSweeney, *Coinminers dogged by mining pool security flaws*, <http://www.coindesk.com/coin-miners-dogged-mining-pool-security-flaws/> [Last visited June 19, 2015].

the robustness of the transactions. For a nascent currency, even a prospect of compromise would have irreversible harms.

In this essay, we argue that the reality is an approximation of the two and perhaps, even more extreme. The 51% threshold is dispositive, but often functions as a smokescreen for the more important debate – that of centralization. Concentration of bitcoins and computing power in a limited number of entities, as shown above, pivots the bitcoin system more towards the “trust-based model” that Nakamoto eschewed. It is pertinent to note that GHash conducted an attempted double spending transaction when it was well below 51%. Thus, how can the horizontal power structure of bitcoins be protected along with its characteristic features? Andreas Antonopoulos opines that the 51% attack hypothesis goes against the fundamental incentives that bitcoin miners have and this makes the attack unlikely.¹⁴ Others have called for reactionary, *ad-hoc* mechanisms such as breaking up groups that reach 51%.¹⁵ The calls for regulation stem from the need to protect the interests of bitcoin investors, the average consumer and the broader economy.¹⁶ At the outset, we argue that both the incentive-based model, premised on the purported incentives of the bitcoin community, and ad-hoc hierarchical measures, such as regulating bitcoin in current regulatory frameworks,¹⁷ are flawed and inadequate. We further compare regulatory regimes across jurisdictions and conclude that regulation targeting the architecture of bitcoin is most likely to be effective in the long-run.¹⁸ For instance, a robust code-based solution strikes the balance between the competing interests outlined so far.

The two broad responses to this problem as they stand, the incentive-based and consequentialist models, merit attention. The incentive-based model relies on the self-interest of the principal stakeholders of bitcoins in protecting the currency.

14 Andreas Antonopoulos, *L.A. Bitcoin Meetup 2014*, January 9, 2014, <https://www.youtube.com/watch?v=bTPQKyAq-DM#t=2942> [Last visited June 19, 2015].

15 Alex Wilhelm, *51% fears rattle the bitcoin community*, <http://techcrunch.com/2014/06/15/51-fears-rattle-the-bitcoin-community/> [Last visited June 19, 2015].

16 Patrick Kirby, *Virtually Possible: How to Strengthen Bitcoin Regulation Within the Current Regulatory Framework*, 93 NORTH CAROLINA LAW REVIEW 189, 206 [2014].

17 For example Kelsey L. Penrose, *Banking on Bitcoin: Applying Anti-Money Laundering and Money Transmitter Laws*, 18 NORTH CAROLINA BANKING INSTITUTE 529 [2014].

18 *Contra* Nikolei M. Kaplanov, *Nerdy Money: Bitcoin, The Private Digital Currency and the Case Against Its Regulation*, 25 LOYOLA CONSUMER LAW REVIEW 111, 167-169 [2012].

For instance, GHash itself stopped new membership and witnessed an outflow of members as it approached 50%. Its press release clarifies that it didn't intend to reach 51% "*as it will do serious damage to the Bitcoin community, which we are part of.*"¹⁹ We argue that that this model is problematic at three levels. *First*, it presumes that all stakeholders have a vested interest in the future of bitcoin. This is not necessarily true. By eluding state regulation *in toto*, bitcoin represents the biggest threat to state monopoly over economic life. Moreover, bitcoin openly challenges state policies. When government pressure compelled Visa and PayPal to block transactions involving Wikileaks, bitcoins were the alternative means of payment. Therefore, the government, which is also a critical bitcoin stakeholder, has an incentive to subvert it from within. Further, the farrago of thefts and fraudulent transactions²⁰ mean a presumption of good faith is at best, fanciful. *Second*, it ignores the possibility of short-term gain. Phenomena like insider trading, predatory pricing and artificial currency devaluation have destabilizing consequences on the financial system but are still popular since they yield high short-term gains for individual stakeholders. This behaviour would and has been mirrored in crypto currencies.²¹ *Third*, a system that is contingent on the benevolence of actors is inherently weak. Any system of accountability is not based on the assumption that the actors are benign, but in the need to curtail the actions of malevolent ones. For instance, even in terms of institutional governance, constitutions are drafted on the basis of the principle of constitutionalism, which stipulates that there be a charter of limitations to governmental power – although the setting up of the government may be a *bona fide* act. Thus for bitcoin to develop, GHash's press release should be inconsequential to say the least.

19 *Bitcoin mining pool GHash.IO is preventing accumulation of 51% of all hashing power*, https://ghash.io/ghashio_press_release.pdf?_ga=1.178723236.1232532447.1402571644 [Last visited June 19, 2015].

20 See for example Joon Ian Wong, *Over \$11 Million Lost in Bitcoin Scams Since 2011*, *Coin Desk*, <http://www.coindesk.com/research-11-million-lost-bitcoin-scams-since-2009/> [Last visited on August 1, 2015]; Nicky Woolf, *Bitcoin 'Exit Scam': Deep-Web Market Operators Disappear with \$12 M*, *The Guardian* <http://www.theguardian.com/technology/2015/mar/18/bitcoin-deep-web-evolution-exit-scam-12-million-dollars> [Last visited on August 3, 2015]; Dante D'Orazio, *Former Mt. Gox CEO Arrested on Claims of Stolen Bitcoins*, *The Verge*, <http://www.theverge.com/2015/8/1/9083989/mt-gox-ceo-arrested-in-tokyo> [Last Last visited on August 3, 2015].

21 *Ibid.*

The consequentialist model calls for intervention after monopolistic actions have taken place. For example, a group that reaches 51% will be compelled to break up before further transactions are allowed. However, a consequentialist reaction is often merely a stop-gap measure and is hardly an adequate response to a principled issue with the system. Legal regulation is consequentialist, as the law comes into force only after a situation demanding regulation arises. Even in the sense of compliance based regulation, for such guidelines to be legislated upon, a situation requiring such legislation may have arisen – or can be predicted to arise in the near future. In that sense, we argue that post-facto fire-fighting is ineffective in the long run, as there will constantly be ways in which code may be used to subvert such regulation. Michael Lewis highlights Regulation NMS that, he argues, not only failed to curb fraudulent trades but also strengthened the position of market intermediaries allowing for unscrupulous high frequency trading. The gap between technology and law would be further widened by rigid consequentialist approaches.

In order to understand emerging trends in regulation of cryptocurrencies, and to highlight the potential issues that may arise, we have undertaken a comparative study of the status of bitcoins in countries that have provided regulatory responses to it.²²

The first pool of countries stands at the twilight of acceptance/regulation of bitcoin. Israel recognized it as a ‘virtual currency’, apt for payments.²³ The Belgian government has legalized but not incorporated it as a valid currency.²⁴ The Hong Kong Monetary Authority decided against regulation of this ‘virtual commodity’.²⁵ Further, Turkey,²⁶ Columbia²⁷ and Denmark prohibit financial institutions from

22 Kashmir Hill, *Bitcoins Legality Around the World*, <http://www.forbes.com/sites/kashmirhill/2014/01/31/bitcoins-legality-around-the-world/> (Last visited on June 19, 2014).

23 Niv Elis, *Bank of Israel mulls regulating, recognizing Bitcoin virtual currency*, <http://www.jpost.com/Business/Business-News/Bank-of-Israel-mulls-regulating-recognizing-Bitcoin-virtual-currency-333894> (Last visited on June 19, 2014).

24 Danny Bradbury, *Belgium's Finance Minister has no objection to bitcoin*, <http://www.coindesk.com/belgiums-finance-minister-has-no-objection-to-bitcoin/> (Last visited on June 19, 2014).

25 Alan Wong, *In Hong Kong, Placing Their Bets on Bitcoin*, New York Times, at http://dealbook.nytimes.com/2014/03/19/in-hong-kong-betting-big-on-bitcoin/?_php=true&_type=blogs&_r=0 (Last visited on June 19, 2014).

trading in cryptocurrencies while individuals face no such restriction. This might change as Denmark prepares standards that protect users from potential risks.²⁸ Germany allows bitcoins to be used for trade and tax, although recognizing bitcoins as “private money”.²⁹

The second pool is of nations with a stringent tax liability mode of regulation. Countries such as Australia intend to establish tax guidelines for bitcoin use.³⁰ Brazil³¹ and Finland³² tax bitcoin transactions as capital gains. Bulgaria, on the other hand, treats bitcoins as financial instruments, thus taxing it at the same rate as ordinary income.³³ Norway treats bitcoins as an asset, attracting wealth and sales tax.³⁴ Canada has issued a statement that details the treatment of bitcoins in the same manner as barter transactions, as well as the applicability of the existing anti-money laundering legislation.³⁵ The UK similarly levies VAT if bitcoins are

26 *Regulation of Bitcoin in Turkey*, <http://www.coinstech.com/regulation-of-bitcoin-in-turkey/> (Last visited on June 19, 2014).

27 Pete Rizzo, *Colombia Stops Short of Bitcoin Ban, Bars Banks From Industry*, <http://www.coindesk.com/colombia-stops-short-bitcoin-ban-bars-banks-sector/> (Last visited on June 19, 2014).

28 Frances Schwartzkopff, *Bitcoins Spark Regulatory Crackdown as Denmark Drafts Rules*, <http://www.businessweek.com/news/2013-12-17/bitcoin-rules-drafted-in-denmark-as-regulator-warns-against-use> (Last visited on June 19, 2014).

29 Matt Clinch, *Bitcoin recognized by Germany as ‘private money’*, <http://www.cnn.com/id/100971898> (Last visited on June 19, 2014).

30 Jon Southurst, *Australia Will Set Official Tax Guidelines on Bitcoin This Year*, <http://www.coindesk.com/australia-official-tax-guidelines-bitcoin-this-year/> (Last visited on June 19, 2014).

31 Kenneth Rapoza, *Brazil Follows IRS, Declares Bitcoin Gains Taxable*, <http://www.forbes.com/sites/kenrapoza/2014/04/07/brazil-follows-irs-declares-bitcoin-gains-taxable/> (Last visited on June 19, 2014).

32 Nermin Hajdarbegovic, *Bitcoin Classified ‘Commodity’ by Finland Central Bank*, <http://www.coindesk.com/bitcoin-classified-commodity-finland-central-bank/> (Last visited on June 19, 2014).

33 Pete Rizzo, *Bulgarian Bitcoin Tax Guidance May Leave Money-Laundering Loophole*, <http://www.coindesk.com/bulgarian-bitcoin-tax-guidance-may-leave-money-laundering-loophole/> (Last visited on June 19, 2014).

34 Saleha Mohsin, *Bitcoins Fail Currency Test in Scandinavia’s Richest Nation*, <http://www.bloomberg.com/news/2013-12-12/bitcoins-fail-real-money-test-in-scandinavia-s-wealthiest-nation.html> (Last visited on June 19, 2014).

35 Tim Kiladze, *Canada to regulate bitcoin in war on dirty money*, THE GLOBE AND MAIL, <http://www.theglobeandmail.com/report-on-business/canada-to-regulate-bitcoin-in-war-on-dirty-money/article16812195/> (Last visited on June 19, 2014).

bought and sold, as well as capital gains tax on profits.³⁶ The USA's fragmented approach, where the IRS treats bitcoins as property and subject to capital gains tax, whilst the Treasury treats it as a currency, renders bitcoins subject to anti-money laundering and anti-terrorist financing legislation.³⁷

The third pool is characterized by overcautious regulation, bordering on antagonism. China and Japan, have banned financial institutions from trading in bitcoins within the country while individuals remain exempt from it.³⁸ Taiwan has warned against the use of bitcoins, and prevented a bitcoin ATM from being built.³⁹ Russia pejoratively terms bitcoins "money substitutes" in a classic institutional response to bitcoin that considers the system to be a segue into criminal networks.⁴⁰ The Reserve Bank of India stated it has no plans to regulate while retaining the extensive right to do so.⁴¹ In a 2014 statement, the Indonesian government declared that bitcoins stand in contravention of extant legislation.⁴² Along similar lines, Iceland prohibits foreign exchange trading in crypto currencies; however Iceland has itself adopted Auroracoins, an 'authorized' crypto currency.⁴³

A comparative jurisdictional approach yields the following issues that plague attempts at state regulation. *First*, the defining characteristic of bitcoin is that it is

37 KMR LLP, *Current US Regulatory Developments*, <http://www.mondaq.com/unitedstates/x/277850/Financial+Services/Bitcoin+Current+US+Regulatory+Developments> (Last visited on June 19, 2014).

38 Joe Weisenthal, *China May Be Preparing Harsh New Regulations On Bitcoin*, <http://www.businessinsider.in/China-May-Be-Preparing-Harsh-New-Regulations-On-Bitcoin/articleshow/33130585.cms> (Last visited on June 19, 2014) ; NerminHajdarbegovic, *Japan decides against bitcoin regulation for now*, at <http://www.coindesk.com/japan-decides-bitcoin-regulation-now/> (Last visited on June 19, 2014).

39 Aries Poon, *Taiwan Rejects Bitcoin ATMs*, <http://blogs.wsj.com/chinarealtime/2014/01/06/taiwan-rejects-bitcoin-atms/> (Last visited on June 19, 2014).

40 Ellis Hamburger, *Russia Bans Bitcoin*, <http://www.theverge.com/2014/2/9/5395050/russia-bans-bitcoin> (Last visited on June 19, 2014). ; Shie Lynn-Lim, *Malaysia's Central Bank Warns of Bitcoin Risks*, WALL STREET JOURNAL, <http://online.wsj.com/news/articles/SB10001424052702303640604579298421040674870> (Last visited on June 19, 2014).

41 Joel Dalais, *India Under Bitcoin Regulation? Or Not?*, at <http://bitcoinmagazine.com/10537/india-bitcoin-regulation/> (Last visited on June 19, 2014).

42 Joon Ian Wong, *Indonesia Central Bank warns against bitcoin use*, at <http://www.coindesk.com/indonesia-central-bank-warns-bitcoin-use/> (Last visited on June 19, 2014).

43 *Crypto: Iceland To Adopt Crypto-Currency*, <http://financialcrimeasia.org/2014/02/12/crypto-iceland-to-adopt-crypto-currency-while-hackers-attack-bitcoin-and-ny-regulations-loom/> (Last visited on June 19, 2014).

a decentralized, accessible currency. The nature of municipal law necessitates an institutional approach to regulation that entails a hierarchical power structure. Such an institution would have the power to restrict circulation or ban bitcoins altogether, thus diminishing its accessibility. *Second*, the regulatory regimes' treatment of bitcoins as a commodity, rather than a currency, betrays a reluctance to engage with decentralized currencies. *Third*, there is a vast information gap on the purposes for which bitcoins are used, which lends itself to suspicion and overcautious regulation. Finally, the clearest issue that emerges is that of incompatibility – that each country has different views on what sort of measures to impose on bitcoins and what sorts of laws they might be subject to, thereby creating no space for compossibility.

Thus there is a dissonance between law's concreteness and certainty, and technology's constant state of innovation. This throws up new challenges for legal regulation that may not be solved simply through the proliferation of new legislations or through the expansion of those in existence. Lawrence Lessig's 'Code' provides a compelling framework in which this constructive may be based.⁴⁴ He lays out four factors, which presently determine to what extent and how cyberspace is regulated: the law; the norms of the society; the market; and the architecture of cyberspace. Lessig argues that in cyberspace, it is not only regulation by law, but the very design of the technology that is the framework for regulation the limiting or regulatory framework. Lessig terms this as the 'architecture of control' of the digital world. He argues that the law exists to regulate the market, and although it has an impact upon technology, code forms the architecture of the system and may subvert the regulatory framework that the law has imposed upon it. For cyberspace to continue existing as it is, it must embody certain values that netizens hold dear – such as free speech, individual control and anonymity.⁴⁵ Since cyberspace is created by servers in different geographical locations, its regulation is complex and cannot be done by one country alone.⁴⁶ Further the application of national laws to different servers, based on their territorial location leads to further complications with regard to say, liability for harmful content, accessed from

44 Lawrence Lessig, *CODE V. 2.0*, 2006.

45 Lawrence Lessig, *Code is Law*, HARVARD MAGAZINE, at <http://harvardmagazine.com/2000/01/code-is-law.html> (Last visited on June 19, 2014).

46 Andrew D. Murray, *THE REGULATION OF CYBERSPACE: CONTROL IN THE ONLINE ENVIRONMENT* (2007).

another territorial location. By virtue of being deeply entrenched in state institutions, law is principally based on different grounds as opposed to the digital space.⁴⁷ Lessig acknowledges this and states that the uniqueness of the interaction that we have through cyberspace, is difficult for the law to adequately regulate. Therefore, in light of Lessig's framework, we propose a two-pronged, principle-based solution that will speak to the idea that the law can exist as a mere tool to correct states of imbalance, as they exist, between the market and code.

The most prevalent issues, as outlined above, are those of centralization and monopolization. Although mining pools provide certain advantages, the threat of monopoly looms large, and questions the survival of the bitcoin project in the first place.⁴⁸ Thus, the first prong of the solution that we propose is that the code itself be altered in order to prevent monopoly creation. For instance, monopolistic behavior such as tending towards 51% would result in being locked out of the bitcoin system altogether. The sanction can operate on a sliding scale depending on the egregiousness of the transgression. Rather than proposing a situation where there exists no system of regulation at all (deregulation), we propose that the primary task of regulation of a complex piece of technology must lie with the creators and coders of the same, so as for them to preserve the values that Nakamoto envisioned.⁴⁹

The second prong is a move towards a threshold that may be introduced within the code, in order to automatically break mining pools the moment they reach a particular limit. This model would only require the code to break mining pools once they reach a particular limit. We are proposing this on a principled level, and are aware that any sort of threshold set would be arbitrary in nature. However, we argue that this is necessary as it would tackle the actual problem of concentration in mining of bitcoins, by keeping it significantly below the level of survival required for bitcoins to continue to remain within circulation, as a cryptocurrency. There exist coded solutions in this form, such as the P2Pool.⁵⁰ P2Pool miners create

47 H.L.A Hart, *THE CONCEPT OF LAW* (1961).

48 Alex Hern, *Bitcoin currency could have been destroyed by 51% attack*, *THE GUARDIAN*, <http://www.theguardian.com/technology/2014/jun/16/bitcoin-currency-destroyed-51-attack-ghashio> (Last visited on June 19, 2014).

49 *Supra* note 1.

50 P2Pool, at <http://p2pool.in/> (Last visited on June 19, 2014).

their own blocks, however share the rewards amongst the entire pool. An internal coded mechanism has been created – each share is assembled into a share chain, in order to maintain fairness and prevent fraud. Thus those miners who do not follow these rules get excluded from the main chain, thereby ensuring that such rules of fairness are followed.⁵¹ This solves the issue of decentralization, as no single person is in charge of the distribution of rewards, as well as retains the autonomy of individual miners who can choose which transactions they want to enter into. Further there exists no reliance upon pool operators and such entities, for payment to miners, as miners get paid directly.⁵²

The two principal ideas in this essay are the harms of centralization in bitcoin coupled with the inevitable institutionalization that accompanies state regulation. We clearly demonstrate that any form of traditional regulation that entails a vertical power structure militates against the very idea of bitcoin itself. Is it possible to protect bitcoin from monopolistic practices while retaining its horizontal, decentralized structure? The balance that is to be struck is that of code, law and the marketplace. Lessig provides the ideal framework to understand how this balance would play out. It speaks to both the futility of centralized regulation in the digital space as well as the dire need to protect its most cherished values. We also add nuance to this balance by proposing two possible solutions, each functioning in a different paradigm. Therefore, we show that it is not only viable but also vital for bitcoin to find this balance, before, to borrow from Douglas Adams, it becomes necessary to wave the towel “*in emergencies as a distress signal, and of course dry yourself off with it if it still seems to be clean enough.*”

51 P2Pool, *Bitcoin wiki*, at <https://en.bitcoin.it/wiki/P2Pool> (Last visited on June 19, 2014).

52 *What is the P2Pool, Bitcoin Stack Exchange*, <http://bitcoin.stackexchange.com/questions/3626/what-is-the-p2pool> (Last visited on June 19, 2014).