Bitcoin: The First Self-Regulating Currency?

Bitcoin: The First Self-Regulating Currency?

Samuel Elliott*

ABSTRACT

This article provides an examination of regulation theory as applied to Bitcoin. Through an examination of the parallels with Ogus' model for self-regulation, it is demonstrated that several unique features inherent to cryptocurrencies offer the benefits of regulatory oversight without the drawbacks. The article also provides a broader socio-regulatory analysis of Bitcoin in an attempt to better understand the benefits of competitive self-regulation for platform users. Finally, this article examines whether cryptocurrencies should be regulated by way of traditional State-based models and, if so, which of these approaches (if any) ought to be used to regulate the platform.

INTRODUCTION

Ogus' model of self-regulation relies on three environmental factors being present: that the activity is affected by some form of market failure; that private law instruments are inadequate or inefficient to correct said failure; and that self-regulation is a better method of resolving the failure than conventional regulation.[1] However, such self-regulation has been conceptualised as all-but-impossible in e-commerce. Our understanding of ownership over intangible goods has been intimately linked to the ability to enforce and alienate our property rights through trusted third parties.[2] Bitcoin has been challenging this conception since its launch.

* Graduate of the London School of Economics (LLM Eur, 2017). Graduate of Dublin City University (BCL Law and Society, 2015) Pre-Trainee at Matheson, Dublin, Ireland (2017). My thanks to Professor Andrew Murray for his assistance in understanding the legal issues surrounding Bitcoin. Further thanks to Killian Mills and Sean Gibbons in helping to conceptualize the technical background to cryptocurrencies.

[1] Anthony I Ogus, 'Rethinking Self-Regulation' (1995) 15 OJLS 97.

[2] Ranging from a bank carrying out an electronic transfer to a Court enforcing ownership of IP rights.

Satoshi Nakamoto[3] published Bitcoin's 'proof of concept' in 2008.[4] Nakamoto notes therein that 'commerce on the internet has come to rely almost exclusively on financial institutions serving as trusted third parties'.[5] He argues that the need for a centralised intermediary creates inherent inefficiencies for the digital transfer of wealth. To address this inefficiency, an alternative system, built upon cryptographic proof rather than trust, was proposed, allowing for direct peer-to-peer transfers without the risk of double spending.[6] Since then, Bitcoin has seen exponential growth among users who are sceptical of State interference and regulation in currency. There is no government, company, or bank in charge of the management of Bitcoin.[7] This, however, neither means that the platform is entirely anarchistic nor that it is unregulated as such. Building on Ogus' model, this article argues that Bitcoin is the first truly self-regulating currency. It resolves a number of inefficiencies within intermediary-based transfers through a decentralised, participatory model of regulation.

Instead, through an examination of Bitcoin's *sui generis* features, we can identify a number of parallels between the participatory currency and traditional regulatory models. We see that Bitcoin is underpinned by an implicit social contract wherein consensus-building and voluntary association replace centralised, rule-based forms of regulation. Thereafter, we will establish what the best means for regulating the platform are, which includes investigating the total deregulation of cryptocurrencies altogether.

---

[3] The creator of Bitcoin – though Nakamoto is widely believed to be a pseudonym. For the sake of convenience, I have assumed Nakamoto to be male throughout this article.

[4] Satoshi Nakamoto, 'Bitcoin: A Peer-to-Peer Electronic Cash System' <https://bitcoin.org/bitcoin.pdf> accessed 28 February 2017.

[5] ibid 1.

[6] Double spending is a problem within digital currencies wherein units of currency, represented as files, may be spent more than once through duplication or falsification of the same. See Usman W Chohan, 'The Double-Spending Problem and Cryptocurrencies' (2017) University of NSW Discussion Papers Series <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3090174> accessed 21 February 2018.

[7] Primavera De Filippi, 'Bitcoin: A Regulatory Nightmare to a Libertarian Dream' (2014) 3 Internet Policy Review <https://policyreview.info/node/286/pdf> accessed 26 April 2017.

I. OGUS' MODEL AND THE STATUS QUO

By examining the first two aspects of Ogus' model, one can see how the failings of the ledger-based status quo paved the way for Bitcoin's success. The market failure inherent in the trust-based model, and the inability of private law and alternative dispute resolution ('ADR') mechanisms to efficiently resolve ownership contentions, is inherently disadvantageous for transferors and transferees alike.

The Inefficiency Problem: Market Failures and the Status Quo

Prior to the invention of blockchain technology, inequality in power between financial service providers and end-users made self-regulation of currency impossible. The need for intermediary bodies and the lack of accessible infrastructure for verification of transfers at the individual level made the centralised system the most efficient method of regulation. However, together, the aforementioned led to a market failure insofar that the digital transfer of wealth became inherently inefficient. Such inefficiency has been compounded by in-house dispute resolution processes and courts serving as the sole method through which ownership conflicts, arising out of the intangible nature of the assets, could be resolved.

Naturally, the exchange of physical assets, eg currency, does not necessitate a third party intermediary. Both parties can immediately verify that the correct transfer occurred and it cannot typically be reversed without legal action or physical force. The tangibility of the goods exchanged serves to verify the transaction. The only real risk of fraud, as regards the currency itself, comes in the form of counterfeiting. There is neither a functional need for an intermediary nor for significant regulation – both parties use a common platform and the only necessary rules are the established property laws within a State.

For distance transactions, both parties face issues of opaqueness. As the exchange of physical goods cannot be easily carried out, a substitute must be used instead. Typically, this manifests in the form of a card payment or digital wire transfer. In other words, there is no physical exchange of value. During these transactions, instead, the intermediary logs the transfer against a ledger of each

party's wealth.[8] Without this trusted ledger, either party could 'double spend' digital currencies by way of repeatedly replicating and alienating them.[9]

However, the intermediary-based system has disadvantages. Nakamoto argues that institutions cannot avoid regulating their platforms and mediating disputes due to the inherently trust-based nature of the model.[10] This, as this paper submits, is the root cause of the lack of permanency in transfers. As responsibility must be vested in the intermediary, it must equally be able to resolve any conflicts that arise, thereby creating inherent inefficiencies in transactions. The intermediary-based system therefore carries three distinct disadvantages for transactors: (1) a lack of efficiency; (2) a lack of immutability; and (3) the potential for interference by the intermediary.[11] These are the key aspects of the market failure that Bitcoin seeks to overcome.

Private Law Issues and Dispute Resolution

The second trigger for public interest in self-regulation is when private law instruments are inadequate or too costly to correct the market failure.[12] Private law is suited to resolve issues relating to physical transfers. The risk of fraud, at least in terms of the currency itself, is relatively low and double spending is non-existent, as each party can instantly verify whether the correct payment (or goods) has been obtained.

Digital transfers present a number of issues for transferors in terms of disputes. Information asymmetry is a problem insofar that the transferee relies entirely on the intermediary to verify the transfer. With the control over the transfer vested in the intermediary, the surety of ownership and of transfer is impossible without reference to the trusted third party. Ensuring that these intermediaries act fairly becomes a matter for State oversight, guaranteeing that the financial market is not paralysed by a lack of trust.

Nakamoto, for example, notes that there is no way to make non-reversible payments for non-reversible services.[13] This creates inefficiencies. Intermediaries,

---

[8] Jerry Brito and Andrea Castillo, *Bitcoin: A Primer for Policymakers* (Mercatus Center at George Mason University 2013) 5.

[9] ibid.

[10] For example, non-reversible payments cannot be made for non-reversible transactions.

[11] Brito and Castillo (n 8) 5.

[12] Ogus (n 1) 97.

[13] Nakamoto (n 4) 1.

possessing total control over their centralised ledger, are also responsible for the establishment of ownership where disputes arise. Private law instruments are, in this instance, a fallback for the attribution of ownership where disputes cannot be resolved though the parties' consent. However, regardless as to how advantageous ADR is in resolving transactional conflicts, there is no absolute guarantee of ownership. Brito, furthermore, notes that the cost of chargeback fraud and the accompanying charges can be a prohibitive barrier to small businesses seeking to enter the digital market.[14]

Digital Currency Pre-Bitcoin

Next, it is worth briefly examining the history of digital currency pre-Bitcoin to contextualise those advancements made to address key issues surrounding decentralisation.

The technology at the heart of cryptocurrencies was envisaged in 1992, when retired physicist Timothy May convened a number of colleagues to discuss decentralising digital currency.[15] Heavily influenced by anarchistic and libertarian philosophy, the group proposed a platform for digital payments beyond the realm of banks, credit card companies, and other intermediaries. Jim Bell, a member of the early cryptography community, posited a thought experiment wherein anonymous digital currency was used to crowdfund 'assassination politics' against unpopular politicians.[16]

Although Bell's paper ultimately resulted in an IRS raid and led the author to be imprisoned for several years, it offers valuable insight into the early motivation of developers like Nakamoto. These developers feared that the newfound freedoms the Internet offered their community would, in time, be curtailed through government oversight and control over spending.[17] Public key encryption and 'digital cash' offered the opportunity to build institutions free from governmental control, wherein the only limit to what could be bought and sold was the physical limits of the providers themselves.

---

[14] Brito and Castillo (n 8) 15.

[15] Morgen E Peck, 'Bitcoin: The Cryptoanarchists' Answer to Cash' (*IEEE*, 30 May 2012) <http://spectrum.ieee.org/computing/software/bitcoin-the-cryptoanarchists-answer-to-cash/0> accessed 3 May 2017.

[16] Jim Bell, 'Assassination Politics' (1992) <http://www.outpost-of-freedom.com/jimbellap.htm> accessed 3 May 2017.

[17] ibid.

It was in 1997 that Nick Szabo developed the first proto-cryptocurrency.[18] Szabo, similar to Bell, started with a thought experiment on what gave gold its value. He drew an analogy between difficult-to-mine gold and difficult-to-solve problems. A puzzle that takes time and energy to solve, with the solution then presented in the form of a digital coin, can be considered valuable in a way similar to gold.[19] As the network built incrementally on resolved puzzles, a chain of solutions – the blockchain – formed, which served the double purpose of also timestamping transactions. The network, unable to proceed to the next puzzle without having answered the preceding, guarded against 'double spending' and 'double mining'.

Szabo's Bit Gold was a departure from the norm of digital currencies. The earlier DigiCash, also based on cryptography, relied on a centralised bank for oversight. Szabo, seeking to replicate gold, envisioned Bit Gold to hold value as a standalone asset. Instead of having their value backed and, thus, arguably generated by banks, cryptocurrencies would be inherently valuable based on the input required to resolve the digital puzzle.

Bit Gold was an imperfect solution for the market issues present within e-commerce. While it did provide some fundamental protection against double spending, the system was based on a quorum of network addresses.[20] Networks, however, are vulnerable to, most importantly in this case, 'Sybil attacks', where an attacker forges a number of network addresses with which they can take control over the network as a whole.[21] This vulnerability prevented widespread adoption of the digital currency, given there was little security against this form of cyber attack. At the time, forging an identity was relatively easy, making a truly decentralised and collaborative means of regulation impossible. It was not until Nakamoto's innovations in blockchain technology that Sybil attacks could be prevented altogether and a secure, decentralised digital currency became possible. These innovations are discussed below.

---

[18] Nick Szabo, 'Bit Gold' (*Unenumerated*, 27 December 2008) <http://unenumerated.blogspot.ie/2005/12/bit-gold.html> accessed 21 February 2018.

[19] ibid.

[20] Nick Szabo, 'Secure Property Tiles with Owner Authority' (*Satoshi Nakamoto Institute*, 1998) <http://nakamotoinstitute.org/secure-property-titles> accessed 3 May 2017.

[21] John R Douceur, 'The Sybil Attack' in Peter Drushel, M Frans Kaashoek and Antony IT Rowstron (eds), *IPTPS '01 Revised Papers from the First International Workshop on Peer-to-Peer Systems* (Springer-Verlag 2002).

II. SELF-REGULATION AS A SOLUTION TO THE STATUS QUO INEFFICIENCIES

To comprehend the significance of the departure from the status quo Bitcoin represents, it is important to understand the technological developments underlying the cryptocurrency. Nakamoto found the core issues within the intermediary model to derive from the need for a trusted third party.[22]

Technical Description of Bitcoin

Rather than representing each transaction using a centralised ledger, Nakamoto created a standalone digital currency. Each Bitcoin is a representation of a chain of digital signatures. Transfers are carried out by digitally signing an algorithmically-generated number, a 'hash', of the previous transaction and the unique public cryptographic key ('public key') of the next owner, and appending this to the previous end of the coin.[23] Public-key cryptography allows each node in the network to verify whether a digitally signed transaction is valid.[24] To prevent double spending, Nakamoto uses a publicly distributed ledger system. The ledger timestamps each transaction within the network, ensuring a coin cannot be repeatedly transacted by one owner – thus solving the double-spending problem.[25] New transactions are broadcast to other nodes within the network, which collate them into a block, hence the label 'blockchain'.

Nodes, then, work on finding a difficult proof-of-work for each block. Once discovered, a new Bitcoin is created and added to the ledger. This requires nodes to discover a value that, when hashed using the SHA-256 algorithm, begins with a string of zero bits – a computationally intensive task whose success is easy to verify.[26] The proof-of-work serves to timestamp transactions and to ensure that the network reaches consensus on which transactions have entered the blockchain. Once a node discovers a proof-of-work, it broadcasts the block to the network. The block, in turn, will only be accepted if all transactions within the block are valid and not double-spent. The latter serves to verify broadcast transactions while simultaneously generating new Bitcoin. It also ensures that

[22] ibid.
[23] ibid 252.
[24] Brito and Castillo (n 8) 5.
[25] Nakamoto (n 4) 2.
[26] This value is called a nonce.

consensus is built amongst the nodes which prevents conflicting ledgers, called 'network forks'.[27] Nodes then create the next block in the chain by using the hash of the accepted block.[28] This process secures the network against attackers, who would have to modify the proof-of-work for every previous transaction within the chain in order to modify the ledger.

As discovering the nonce is computationally intensive, Bitcoins are inherently scarce. There is no central authority to distribute them. Instead, wealth is generated through contributing to the maintenance of the network. Furthermore, if the output value of a transaction is less than the input value, a transaction fee can be added to the incentive value of the block containing the transaction.[29] This allows the platform to remain viable after the last Bitcoin is 'mined'.[30] Every 210,000 blocks, the value of creating a new block is halved, limiting the supply of Bitcoins over time.[31]

The network will analyse the time taken to mine 2016 blocks periodically. The problem difficulty will then be adjusted to ensure that mining those blocks takes close to two weeks to complete. Doing so ensures that Bitcoin are mined at a manageable pace despite the advances in processing power that become available to miners. As such, Bitcoin retains its value in response to external factors like Moore's law[32] and developments in hardware.[33]

---

[27] Nicolas Houy, 'The Bitcoin Mining Game' (2016) 1 Ledger 53. Network forks have happened – both intentionally and unintentionally – a number of times during Bitcoin's lifespan.

[28] Nakamoto (n 4) 2.

[29] ibid.

[30] Once 20,999,999.9769 Bitcoins have been added to the Blockchain, the currency will become entirely reliant on transaction fees to maintain the ledger. This is estimated to happen circa 2140.

[31] Jocab Donnelly, 'What is the 'Halving'? A Primer to Bitcoin's Big Mining Change' (*coindesk*, 12 June 2016) <http://www.coindesk.com/making-sense-bitcoins-halving> accessed 26 April 2017.

[32] Moore predicted that the number of circuit components that can be arranged on an integrated chip would double in number year on year. To date, Moore's Law has served to predict the exponential growth in processing power of modern hardware relatively well. See Chris Mack, 'The Multiple Lives of Moore's Law' (2015) 52 IEEE Spectrum 31.

[33] For further background information, see the discussion on Stackexchange <https://bitcoin.stackexchange.com/questions/5838/how-is-difficulty-calculated> accessed 23 February 2018.

Ogus and Bitcoin: Is Bitcoin Self-Regulating?

Retuning to Ogus, we can examine whether Bitcoin falls within the model of a self-regulating entity.[34] Thereafter, the effectiveness of Bitcoin to resolve the market failure within intermediary transactions can be scrutinised.

Ogus argues that there is a 'multitude of institutional arrangements which can properly be described as self-regulation'.[35] He rejects the traditionalists' view, limited to a Self-Regulating Authority ('SRA') removed from the body politic, as too narrowly conceived. Instead, Ogus holds there to be a self-regulatory spectrum, ranging from bodies being entirely self-regulating to public regulation.[36] At one extreme, self-regulating bodies may be subject to government oversight. At the other, these may be entirely independent and private.[37] Furthermore, the rules could be formally (legally) binding or purely voluntary. Finally, regimes can be monopolistic or voluntary. The main difference between a self-regulating and publically regulated model is, therefore, the origin of rulemaking within a system – the enforcement and effect of these rules thereafter can vary.

Bitcoin steps beyond Ogus' conception of self-regulation insofar as it surpasses the need for a centralised authority altogether. The distributed ledger, moreover, provides security of ownership and guarantees against fraud. Rather than having fiscal controls on the creation of new currency, Bitcoin automatically reduces the output of mining over time at a predetermined rate.

Transactions are verified and encoded into the blockchain through a participatory community model wherein consensus is built amongst the network. Such a verification system departs from the traditional regulatory model and Ogus' conception of an SRA. Basic rules of ownership and the transfer of assets are not enforced by a court or regulator, but instead by nodes through the codification of the ledger.[38] Participation is encouraged through the reward of new Bitcoins, thereby creating a feedback loop of wealth creation and currency management.[39]

---

[34] Ogus (n 1) 97.
[35] ibid 99.
[36] ibid 100.
[37] ibid.
[38] Houy (n 27) 53.
[39] ibid. Houy's article reflects on Bitcoin mining through the lens of game theory, which provides context as to the motivations for each individual miner.

However, whilst enforcement is decentralised, decision-making is not. Although Bitcoin's codebase is open source, Nakamoto made many of the key decisions as to how the platform ought to operate.[40] Following Nakamoto's retirement in 2010, governance of the codebase was handed to Gavin Andresen, who created the non-profit Bitcoin Foundation thereafter.[41] Thus, while Bitcoin might be decentralised in terms of participation, the development and direction of the project has been centralised in a limited number of developers, resulting in a number of controversial decisions, including forks in the codebase in 2015 and 2017.[42]

Competitive Self-Regulation and Forks in the Codebase

The Bitcoin Foundation can be viewed as analogous to an SRA. When a user forks the codebase, they create a platform that competes with Bitcoin Core. The original platform, however, is unaffected in terms of its functionality. Use of the new platform is entirely optional, giving transferors the ability to use whichever cryptocurrency they feel is most suitable for their needs. Here, one can draw a parallel with Ogus' commentary on competitive self-regulation.[43] Ogus asserts that the principal objection to SRAs is their ability to exploit their monopolistic control of the regulatory environment.

Ogus' solution was to allow for competition between different regimes, thus formulating standards that 'meet consumer preferences at lowest cost'.[44] He finds inspiration in the Coase Theorem, which demonstrates that allocative

---

[40] Matt Odell, 'A Solution to Bitcoin's Governance Problem' (*techcrunch.com*, 21 September 2015) <https://techcrunch.com/2015/09/21/a-solution-to-bitcoins-governance-problem/> accessed 26 April 2017.

[41] Jon Matonis, 'Bitcoin Foundation Launches to Drive Bitcoin's Advancement' (*Forbes*, 27 September 2012) <https://www.forbes.com/sites/jonmatonis/2012/09/27/bitcoin-foundation-launches-to-drive-bitcoins-advancement/#7903735d8683> accessed 26 April 2017.

[42] Alex Hern, 'Bitcoin's Forked: Chief Scientist Launches Alternative Proposal for the Currency' *The Guardian* (London, 17 August 2015) <https://www.theguardian.com/technology/2015/aug/17/bitcoin-xt-alternative-cryptocurrency-chief-scientist> accessed 26 April 2017; Jack Crosbie, 'When Will Bitcoin Fork, and What's It Mean for Crypto's Future?' (*Inverse Innovation*, 26 July 2017) <https://www.inverse.com/article/34693-bitcoin-hard-fork-soft-fork-explained-august-1> accessed 1 December 2017.

[43] Ogus (n 1) 103.

[44] ibid.

efficiency will be achieved through voluntary market transactions, regardless of how the law is formulated.[45] This allocative efficiency is subject to transaction costs and to externalities such as, for example, market interests among participants.[46]

A sufficiently talented programmer, or group thereof, can modify the source code of Bitcoin to create a hard fork in the platform.[47] Forking the Bitcoin codebase creates two parallel blockchains, containing both the original and the new coins mined thereafter. Forking allows for competition among offshoots of the project. This allows for preferred platforms, with modified rules on the creation and governance of digital currencies, to prevail over less efficient competitors.

As costs relating to creating and migrating to a different fork are minimal, if not absent, there are no practical barriers to those users unhappy with the established rules. However, as Bitcoin is mined using processing power, a forked offshoot requires continued user investment to remain sustainable. If a currency cannot achieve critical mass, it is unlikely to be successful. Externalities, usually in the form of disagreements amongst the userbase, have caused several offshoots of the network to fail to reach this critical mass.[48]

Decentralisation of Regulation, Black, and Ogus

Black argues that the State is not the sole source of regulation and deems regulation to be inherently limiting, given that there are a number of sources that produce similar rulemaking with similar influence over behaviour.[49] She identifies three generally accepted understandings of what regulation entails. In the first, regulation equates to 'the promulgation of rules by government, accompanied by mechanisms for monitoring and enforcement'.[50] The second conceptualises regulation as any form of direct State intervention in the economy. In the third

---

[45] ibid 100.

[46] ibid.

[47] Amy Castor, 'A Short Guide to Bitcoin Forks' (*coindesk*, 27 March 2017) <http://www.coindesk.com/short-guide-bitcoin-forks-explained/> accessed 28 April 2017.

[48] Bitcoin XT – by way of example – was a 2015 fork that failed to attract critical mass, despite resolving a number of inherent technical issues within Bitcoin core.

[49] Julia Black, 'Critical Reflections on Regulation' (2002) CARR Discussion Papers DP 4 <http://eprints.lse.ac.uk/35985/1/Disspaper4-1.pdf> accessed 28 April 2017.

[50] ibid 8.

sense, regulation extends to all mechanisms of social control or influence affecting all aspects of behaviour from whatever source.[51]

The first two conceptualisations of regulation exclude private rulemaking by nature. The third is more inclusive, but risks being so expansive that it renders the definition moot. If any form of influence is regulation, then framing the term becomes effectively pointless. Black restricts the third definition by noting the implicit understanding that regulation targets economic actors.[52] She builds on Ogus' argument that regulation is best understood 'by reference to different systems of economic organization and the legal forms which maintain them'.[53]

Instead of framing regulation as a directive system, of commands backed by sanctions, we can understand it as facilitating the market.[54] It provides a set of 'formalised arrangements with which individuals can "'clothe" their (…) relationships'.[55] This conceptualisation of regulation allows for decentralisation. Regulation is understood as rulemaking that influences markets in terms of providing convergent standards for the actors therein. Ogus argues that this definition falls short insofar that it ignores the role the State plays in facilitating the existence of such a system.[56] Such a definition cannot properly describe the role that regulation plays in governing market behaviour by itself, as 'traditional law' serves to provide the stability necessary for the market to exist in the first place.

The parameters under which nodes recognise the creation and transfer of Bitcoin can be understood under Ogus' incomplete definition. Akin to more traditional forms of regulation, these rules provide a means by which users can recognise the creation and ownership of wealth. The network remains functional by requiring users to contribute CPU power to adding transactions to the blockchain. Likewise, the self-adjusting parameters by which the network moderates the creation of new blocks ensure stability of price by creating scarcity. These 'regulations' ensure that Bitcoin remains stable, functional, and valuable.

Similar to Black's first conception of regulation, there is a clear body tasked with the monitoring and enforcement of these rules across the platform.

---

[51] ibid.
[52] ibid 10.
[53] Anthony I Ogus, *Regulation: Legal Form and Economic Theory* (OUP 1994) 1.
[54] ibid 2.
[55] ibid.
[56] ibid 3.

However, rather than having a single centralised body for enforcement, Bitcoin tasks every node on the network with transactional verification, ie whether transactions have followed the 'regulations' that render them valid.

It is arguably difficult to conceptualise 'rulebreaking' within the context of cryptocurrencies. Functionally, double spending is not possible, as nodes within the network will simply refuse to recognise such transactions. If one opts to participate, users are bound by the rules of the platform.

The Social Contract and the Blockchain – Bitcoin as a Sovereign

Reijers, O'Brolcháin and Haynes argue that blockchain governance parallels traditional governance in terms of legitimacy.[57] Examining the Hobbesian 'state of nature', the authors hold that the foundation of the blockchain is built upon isolated individuals of roughly equal power and capacity.[58]

Hobbes' 'state of nature' considers life without government. Therein, the world is one of 'perfectly private judgement' wherein no one agency is authorised to resolve disputes or enforce decisions.[59] He argues that man is subject to uncertainty in terms of other man.[60] This prevents individuals from properly realising their wants and needs in societal terms. In terms of rational self-interest, humans can see that there is both an individual and collective good when it comes to peace seeking and the authority from which it derives. Through recognising and formally realising principles of natural law as a collective, authority is imbued with institutional legitimacy. The end result is a sovereign body, comprised of individuals following a common authority, sacrificing the 'right of nature' (of pure liberty) to institutionally recognise the law of nature.[61]

The intermediary system mirrors the Hobbesean state of nature. Property can only exist in terms of a sovereign power capable of ensuring equal terms among its users.[62] Although e-commerce platforms are not sovereign in terms of power, these do maintain total technical control over the property of others and

---

[57] Wessel Reijers, Fiachra O'Brolcháin and Paul Haynes, 'Governance in Blockchain Technologies & Social Contract Theories' (2016) 1 Ledger 134.

[58] ibid 138.

[59] Sharon A Lloyd and Suzanne Sreedhar, 'Hobbes' Moral and Political Philosophy', *The Stanford Encyclopedia of Philosophy* (2014) <https://plato.stanford.edu/entries/hobbes-moral/> accessed 1 May 2017.

[60] Thomas Hobbes, *Leviathan* (first published 1651, Penguin 1985) ch 13.

[61] ibid chs 17-31.

[62] Equal terms here means equity in the ability to alienate and receive property rights.

are, in turn, governed by a State that derives its legitimacy from individuals. Contemporary platforms serve as an answer to the Hobbesean state of nature that was the commerce on the early Internet. Individuals relied on representative ledgers to provide verification of and arbitration in transactions. However, as this exists as a private service, the State is empowered with regulatory oversight. This provides weak legitimacy to a platform we recognise it as reliable and subject to rules of basic fairness, but at the cost of inefficiencies within the system. By way of example, disputes must be resolved through a consent-based dispute settlement process, an Ombudsman, or the court system. This also creates a lack of absolute surety in ownership, as there is no physical asset actually possessed. The digital wealth exists solely as a record in the intermediary's ledger.

Bitcoin changes the individual's power in terms of the creation, ownership, and alienation of property rights. A sovereign entity is no longer necessary to guarantee these rights. Instead, by way of the functionality of the blockchain, any user can create and enforce property rights over Bitcoin. Users can alienate property with an absolute guarantee that ownership will be given to the transferee. Just as the individuals in Hobbes' state of nature recognise sovereignty, users of Bitcoin recognise Nakamoto's platform as providing this governance.

Whilst it has been demonstrated that blockchain can exist parallel to traditional intermediary governance, we must examine whether it is functionally 'better' than the status quo. In terms of legitimacy, blockchain removes the effect of indirect governance. The network is operated and enforced by the users rather than through a democratic or technocratic system of government. It operates more akin a mandatory social contract, wherein inherently agreed upon terms within the system can be accepted simply by participating therein.

Rather than subjecting users to the alienation of individual control inherent in the intermediary system, the decentralised nature of the blockchain allows absolute permanence and control over currency. The network exists subject only to the platform maintaining a base level of participation. As the generation of wealth actively requires the network to be powered, there remains a demand-incentive to contribute to the administrative tasks that facilitate transactions. The effective removal (or great reduction) of cost at the individual level provides for vastly more direct and efficient means by which property rights can be expressed. However, it should be noted that the increase in popularity in

Bitcoin in late 2017 resulted in mining becoming exponentially more resource-intensive (especially as regards electricity and hardware usage).[63]

The core aspect of 'legitimacy' in terms of e-commerce platforms is the ability to efficiently facilitate the transfer of property. Bitcoin derives its legitimacy through the guarantee, through cryptography and decentralisation, that individuals can express their rights. An intermediary system relies on legitimate State enforcement of the law, expressed through control over providers. It is arguable that the blockchain provides more immediate and effective 'legitimacy', as it removes human inefficiency of transfers. The digital transfer of wealth is fully vested in the individual, rather than being granted by an intermediary.

It is useful to briefly examine O'Dwyer's analysis of Bitcoin as a commons.[64] O'Dwyer argues that 'contribution to the blockchain doesn't only produce money, it also reproduces the community, strengthening a community of trust'.[65] As the network is protected against cyber attacks due to the increasing complexity of the blockchain, it derives legitimacy from participation. The network, in other words, is insulated by the users themselves rather than by a Hobbesean Leviathan or other centralised figure.

III. REGULATING BITCOIN – SHOULD WE?

Having established the models of legitimacy vested in theoretical regulatory regimes, we can now turn to the practical aspects of Bitcoin regulation. Brito, in this regard, warns that Bitcoin 'exists in something of a legal grey area'.[66] It neither fits in current statutory definitions of currency nor have policymakers been quick to implement practical controls regulating the purchase and use of Bitcoins.

---

[63] Peter Fairley, 'Blockchain World - Feeding the Blockchain Beast: If Bitcoin Ever Does Go Mainstream, the Electricity Needed to Sustain it Will Be Enormous' (2017) 54 IEEE Spectrum 10.

[64] Rachel O'Dwyer, 'Other Values: Considering Digital Currency as a Commons' (RGS-IBG Panel: From Co-production to Alternative futures: Creating Cracks: Value, Commons and Alternative Economy, London, September 2014) <https://www.academia.edu/10958178/Other_Values_Considering_Digital_Currency_as_a_Commons> accessed 23 February 2018.

[65] ibid 4.

[66] Brito and Castillo (n 8) 22.

Brito compares the regulatory discourse during the early days of VoIP technology to the contemporary debate on cryptocurrencies.[67] Early VoIP technology, so too, fell beyond the regulatory scope of the US Federal Communications Commission ('FCC'). The technology competed with a highly regulated but technologically limited legacy network. Like Bitcoin, VoIP provided a cheap, direct, and unregulated means for individuals to interact peer-to-peer.

Both Congress and the FCC struggled to respond to the emergent technology in terms of policy decisions. However, by charting a path that clarified the regulatory ambiguity whilst avoiding saddling VoIP providers with a heavy regulatory burden, the technology has flourished. Competition, moreover, has been restored to a stagnant market, lowering costs and providing increased efficiency for end-users. Brito argues that a similar approach ought to be taken for cryptocurrency regulation.[68]

To appreciate the particulars of a regulatory model, however, we must examine the power struggle between the inherently decentralised network of the blockchain, on the one hand, and centralised regulators, on the other. Bitcoin in particular has seen early attention from a number of regulators, including the European Parliament[69] and the IMF.[70] As these bodies seek to bring the network within the prerogative of oversight applied to the more traditional financial bodies, a number of functional and political challenges present themselves.

Justifying Centralised Regulation

Proponents of centralised oversight over Bitcoin lean toward a few models of regulation in particular; either arguing for absolute regulatory control, akin a fiat currency, or for hybridised models of oversight. In establishing where this balance should fall, regulatory proponents typically look to a discreet set of benefits and

---

[67] ibid 23.

[68] ibid.

[69] Christian Scheinert, 'Virtual Currencies: Challenges Following Their Introduction' (2016) European Parliamentary Research Service PE 579.110 <http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/579110/EPRS_BRI(2016)579110_EN.pdf> accessed 1 May 2016.

[70] Dong He and others, 'Virtual Currencies and Beyond: Initial Considerations' (2016) IMF Staff Discussion Note SDN/16/03 <https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf> accessed 1 May 2016.

risks.[71] The IMF, for example, recognises the driving force new technology possesses and understands the appeal of direct peer-to-peer to technology for the financial sector, given the cost advantages of eliminating central clearinghouses. Likewise, the IMF realises the broader benefits distributed ledger technologies can have to strengthen financial efficiency in terms of cross-border – and other traditionally costly – transactions.[72]

However, the IMF similarly identifies a number of negative consequences of cryptocurrencies, namely: money laundering, terrorist financing, and tax evasion through cryptocurrency platforms.[73] Turpin argues that the decentralised nature of the currency, alongside the legal ambiguity within which it operates, has made it particularly attractive for illegal transactions.[74] The relative ease by which evidence of ownership can be disguised created a market for Bitcoin laundering (or 'tumbling') services on the dark web.[75]

Soska and Christin's analysis of darknet markets provides some insight into the economic motivations for law enforcement oversight.[76] The Silk Road, before its takedown, grossed approximately $300,000 per day.[77] The authors further note that there is high mobility for vendors in terms of accessing various sites. With no barrier to 'opening up shop' on several marketplaces, it is common practice for vendors to hedge their bets against takedowns or other errors.[78]

This in mind, it is understandable that Bitcoin has attracted much regulatory and law enforcement attention. The significance of the transactions facilitated, its pseudonymous nature, and the relative difficulty of removing

---

[71] ibid 6.

[72] ibid.

[73] Danton Bryans, 'Bitcoin and Money Laundering: Mining for a Successful Solution' (2014) 89 Ind L J 441.

[74] Jonathan B Turpin, 'Bitcoin: The Economic Case for a Global, Virtual Currency Operating in an Unexplored Legal Framework' (2014) 21 Ind J Global Legal Studies 335.

[75] ibid. Notably, the Silk Road (before closure) had automatic Bitcoin tumbling to break the link between the purchaser and supplier of contraband bought on the site.

[76] Kyle Soska and Nicolas Christin, 'Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem' (USENIX Security Symposium 2015, Washington, DC, August 2015) <https://www.andrew.cmu.edu/user/nicolasc/publications/SC-USENIXSec15.pdf> accessed 2 May 2017.

[77] ibid 8. Totalling more than $100 million a year.

[78] ibid 11.

entrenched darknet markets without a means of controlling their income, makes such interest reasonable. The logical step, in terms of preventing illegal activity, would be to have some form of oversight. However, such an approach has a number of inherent problems.

Difficulties in Centralised Regulation

The inherent difficulties in monitoring transactions that use Bitcoin have been noted by the Federal Bureau of Investigation ('FBI').[79] Of particular concern was the lack of a centralised body to carry out due diligence, monitoring and reporting of suspicious activity, anti-money laundering compliance, and the receiving and processing of legal requests – the primary means by which US regulatory bodies maintain oversight over financial institutions.[80] This represents an intelligence gap for law enforcement insofar that the latter remains reliant on reporting and traditional compliance roles to detect financial crime.

Even though some oversight is possible through the regulation of Bitcoin exchanges, such supervision remains subject to its jurisdictional limits. This approach, furthermore, relies on Bitcoin exchanges falling within the definition of a 'money transmitter' under Federal and State law.[81] Finally, supervision is limited in that it only works when users actually use the exchange – mining and spending Bitcoin is possible without using these services.

Identifying users on the network remains a work-intensive process. Reid and Harrigan managed to identify users by statistically analysing the data sets attached to the blockchain alongside user postings of public-private keys.[82] This method is imperfect, relying on user error rather than weaknesses in cryptocurrencies, and can be safeguarded against by using laundering or tumbling techniques. Overall, the statistical approach is too impractical for consistent law enforcement usage beyond specific high-priority instances.

---

[79] FBI Directorate of Intelligence, 'Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity' (24 April 2012) <https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf> accessed 2 May 2017.

[80] ibid 5. See also FBI, 'White Collar Crime' <https://www.fbi.gov/investigate/white-collar-crime> accessed 2 May 2017.

[81] 18 USC §1960 – Prohibition of unlicensed money transmitting businesses.

[82] Fergal Reid and Martin Harrigan, 'An Analysis of Anonymity in the Bitcoin System' in Yaniv Altshuler and others (eds), *Security and Privacy in Social Networks* (Springer 2013) 197.

Even traditional responses to illegal activity (eg seizures) are much more difficult to effectuate once cryptocurrencies are involved. Transferring Bitcoin out of a wallet requires the corresponding private key. In other words, it either requires the cooperation from the wallet owner or access to a source containing the key, ie, a physical or digital record of it.[83] When an FBI operation closed the Silk Road in 2013, approximately 26,000 Bitcoins held in escrow on the site could be seized and transferred to the FBI's wallet. However, the 600,000 Bitcoins stored in the personal wallet of alleged site operator Robert Ulbricht could not be accessed.[84] This renders approaches such as asset freezing or seizure insufficient, given the impossibility of alienating Bitcoin ownership without access to a user's private key. On top of that, various levels of protection exist worldwide in terms of States' abilities to compel individuals to provide passwords.[85]

This difficulty in enforcement of financial controls has resulted in a number of countries making the purchase and use of Bitcoin illegal.[86] The Central Bank of Bolivia, for example, stated that it is 'illegal to sue any kind of currency that is not issued and controlled by a government or authorized entity'.[87] Likewise, Bangladesh banned cryptocurrencies under the country's strict anti-money laundering regime.[88] While cryptocurrencies largely exist in a legal void, under-resourced States may seek to outlaw them rather than resorting to costly or labour-intensive means of regulating transactions.

---

[83] Robert McMillan and Cade Metz, 'The Ultimate Bitcoin Question: Can the Feds Spend $3.3M in Seized Digital Currency?' (*Wired*, 10 August 2013) <https://www.wired.com/2013/10/silk-road-bust/> accessed 2 May 2017.

[84] Known by the handle 'Dread Pirate Roberts'.

[85] Nathan Saper, 'International Cryptography Regulation and the Global Information Economy' (2013) 11 NW J Tech & Intell Prop 673.

[86] AFP, 'Why Bangladesh Will Jail Bitcoin Traders' *The Telegraph* (London, 15 September 2014) <http://www.telegraph.co.uk/finance/currency/11097208/Why-Bangladesh-will-jail-Bitcoin-traders.html> accessed 4 May 2017; Anthony Cuthbertson, 'Cryptocurrency Round-Up: Bolivian Bitcoin Ban, iOS Apps & Dogecoin at McDonald's' *International Business Times* (New York, 20 June 2014) <http://www.ibtimes.co.uk/cryptocurrency-round-bolivian-bitcoin-ban-ios-apps-dogecoin-mcdonalds-1453453> accessed 4 May 2017.

[87] Cuthbertson (n 86).

[88] 'Why Bangladesh Will Jail Bitcoin Traders' (n 86).

Should Bitcoin Be Regulated as a Currency?

The difficulties in enforcement and regulation are reflective of the lens through which cryptocurrencies are viewed. The FBI criticises the currency, viewing it as a financial instrument or asset, rather than a *sui generis* currency. Brito asserts that this is due to the unique nature of Bitcoin, wherein it can be conceived of as either commodity or currency (or both).[89] It would be unforeseeable – and so too hugely controversial – if a regulatory body were to attempt to oversee every form of transaction, both physical and digital, using a traditional currency. However, given the nature of Bitcoin as 'physical-virtual', this is exactly what is frequently proposed in calls to regulate it. As currency can be generated, moved, and stored across the entirety of the userbase without significant cost, attempting to regulate Bitcoin as a commodity is moot.

He and colleagues argue that cryptocurrencies fall short of the legal concept of currency or money.[90] The legal concept of currency is inherently tied to the power of a sovereign to build a legal framework for issuing banknotes and coins. Likewise, the authors argue that the power of the State to regulate the monetary system is a key feature of 'legal money'. However, He and colleagues' conception draws an arbitrary distinction between a number of features within cryptocurrency systems have that mirror the role of the State. Coins are still issued, albeit based on a collaborative exercise rather than the instructions of a sovereign. Rather than a legal framework surrounding the issuing of money, cryptocurrencies use computational power to regulate the creation of wealth. The network regulates the rate at which wealth is created through responsively adjusting the difficulty of mining. Further regulation is also possible. However, the network refuses to adopt it by continuing to use the Bitcoin Core platform rather than a forked project. Therefore, Bitcoin has the sovereign and regulatory model of a traditional currency – it is merely distributed amongst the entire userbase.

Kaplanov explores a model wherein Bitcoin is treated as a legal alternative currency.[91] He notes that, should this approach be adopted, Bitcoin would have parallels in other community currency systems across the US.[92] Following *Biscoe v*

---

89 Brito and Castillo (n 8) 56.

90 He and others (n 70) 16.

91 Nikolei M Kaplanov, 'Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation' (2013) 25 Loy Consumer L Rev 142.

92 ibid. By way of example, Ithica HOURS or Time Dollars.

Bank of the Commonwealth of Kentucky,[93] the limits of the constitutional prohibition on the issuance of 'bills of credit' was drawn at the State level. Private persons, private partnerships, and private corporations remained unaffected in terms of their ability to create *de novo* currencies.[94] Bitcoin, as a community regulated cryptocurrency, fits comfortably within the legal framework for a private currency within Federal law. However, Kaplanov points out that a number of States limit the use of alternative currencies – eg to prevent employees from being paid through a voucher system.[95]

If we view Bitcoin through the lens of traditional currencies, it can be regulated under US foreign currencies regulation. Doing so would distinguish Bitcoin from other securities and would allow parties to register as foreign exchange dealers or futures commission merchants.[96] In being treated as foreign currency, it would be regulated, but not be subject to the significant regulatory burden that couples domestic currency or securities. This approach implicitly recognises the nature of cryptocurrencies as regulated by the community rather than a centralised body and would see acceptance at the State level of self-regulation. If Bitcoin is treated as a foreign currency, it is reasonable to argue that attempting to regulate the currency at the State level would be acting ultra vires. However, this relationship requires Federal deference to the participatory model. Instead of regulating, it requires the State to accept that the platform itself will regulate and that all decisions ultimately vest in the userbase.

The Argument for *De Minimis* or No Regulation

Kaplanov argues that there is a simple answer to address the friction between regulation and cryptocurrencies: deregulation.[97] He argues that Nakamoto's motivations – eliminating third-party inefficiencies, ease of storage and transport, inherent protection against forgery, and anonymity for the userbase – are the key advantages that drive users to use cryptocurrencies.[98] Each of these advantages is

[93] *Biscoe v Bank of the Commonwealth of Kentucky* [1837] 36 US 257.
[94] ibid.
[95] Kaplanov (n 91) 142.
[96] ibid 149.
[97] ibid 126.
[98] ibid.

tied directly to issues within the trust-based model, which is propagated through State and private actors being reliant upon controlling the status quo.[99]

Kaplanov examines a number of arguments presented against a heavily regulated market for Bitcoin in the US. Outlawing Bitcoin remains difficult. Being an open-source project, there is no company to raid, no persons to subpoena, or no one location to shut down.[100] Likewise, taking down the website and removing the source code would do nothing to affect the underlying decentralised network.[101] The only way to prevent the network from functioning at a technical level would be to remove all nodes from operation. Simply outlawing use of the platform itself would prove inadequate to prevent usage. Kaplanov argues that shutting down Bitcoin 'would likely be very similar to the efforts done to stop online file-sharing programmes'.[102] Efforts to shut down other peer-to-peer platforms have resulted in a largely unsuccessful arms race, wherein underlying features of programmes were tweaked to ensure compliance with rulings, while regulatory aims remained unfulfilled.[103] This is particularly relevant for Bitcoin given its open-source nature and the forking of its codebase. It is unlikely that efforts to heavily regulate or shut down the platform be met with any permanent success.

Kaplanov goes on to argue that the best approach to Bitcoin regulation is to 'allow the market [to] determine whether or not [it] survive[s]'.[104] Cryptocurrencies have contributed to substantial growth in e-commerce, resolving a number of traditional issues in payment platforms in the process. Illegal activities aside, there are a significant number of legal exchanges and markets providing a range of services related to the platform.[105] Kaplanov notes that, despite volatility, the userbase of Bitcoin demonstrates a demand for an

---

[99] ibid 128-129.
[100] ibid 168.
[101] ibid.
[102] ibid 167.
[103] M Eric Johnson, Dan McGuire and Nicholas D Willey, 'The Evolution of the Peer-to-Peer File Sharing Industry and the Security Risks for Users' (41st Hawaii International Conference, Waikoloa, HI, 7-10 January 2008) <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.482.1338&rep=rep1&type=pdf> accessed 21 February 2018.
[104] Kaplanov (n 91) 171.
[105] See 'Trade' (*Bitcoin Wiki*) <https://en.bitcoin.it/wiki/Trade> accessed 5 May 2017.

alternative currency not tied to government control or influence.[106] Kaplanov's approach can be compared to Hayek's in the *Denationalisation of Money*, where the latter argues that competition among private currencies would ultimately guarantee a stable purchasing power and eliminate those less stable currencies from the market.[107]

The social contract and self-regulatory models of Bitcoin have imbibed legitimacy in the currency for the userbase. The platform is not based on trust vested in a sovereign or a body under sovereign oversight, but on that of the users themselves. Every member of the network can verify that the platform is fair, egalitarian, and contributory. Such equality boosts trust in a network where traditional currencies may suffer.[108] The participatory nature of the platform, furthermore, increases its strength as more users adopt it. Camera, in this regard, argues that unified monetary systems are a public good, promoting trade between individuals.[109] However, should a number of currencies develop in parallel, all are devalued, with the userbase fragmenting. Therefore, the best 'win-state' for society is to have a single currency with as large a userbase as possible. This is the root logic under which State-based regulatory models for currency develop. Cryptocurrencies arguably present the next step in developing monetary systems that operate cross-border, wherein ownership is non-ambiguous by nature and instant transmission is allowed without the use of an intermediary.

Rather than viewing Bitcoin as a hostile development that threatens traditional currencies, regulators should instead view it as an innovative next-generation currency. It is in the best interest of policymakers to do so; Bitcoin and other cryptocurrencies will always maintain a market among illegal vendors, but a favourable regulatory environment allows them to be predominantly used by legitimate users. The larger the userbase, the greater the economic gains derived from use of the currency.

---

[106] Kaplanov (n 91) 172.

[107] Friedrich A Hayek, *Denationalization of Money – The Argument Refined* (3rd edn, Institute of Economic Affairs 1990).

[108] Gabriele Camera, 'A Perspective on Electronic Alternatives to Traditional Currencies' (2017) 1 Sveriges Riksbank Econ Rev 126.

[109] ibid 130.

CONCLUSION

In August 2017, Bitcoin's exchange rate with the US Dollar passed $1400.[110] This spike in value came as the Japanese cabinet approved a series of bills to facilitate the use of virtual currencies.[111] These bills, effectively, rendered Bitcoin a legal means of payment. The spike in value associated with favourable sentiment surrounding regulation can be contrasted with the drop in value following announcements that the Chinese Government is to heavily restrict trading platforms for Bitcoin and other 'altcoins'.[112] What this clearly indicates is that the rising value of Bitcoin is directly tied to consumer confidence concerning its use. Through favourable regulatory developments worldwide, the value of the currency has continued to grow. Not only has this increased Bitcoin's legitimacy, it also has transformed the currency from a mere technical project into a major contender with traditional currencies.

Deregulation is the most effective model for States to approach cryptocurrencies. A parallel approach, wherein traditional currencies and digital currencies can coexist, allows both to flourish based on their own merits. The intermediary-based system of e-commerce is inherently inefficient and allowing cryptocurrencies to compete with them on the digital market provides significant benefits to consumers.

Ongoing development of the platform (and community) remains precariously reliant on international regulatory responses. Both the EU and US have taken tentative forays into recognising Bitcoin's benefits. However, a proper legal framework for trade in cryptocurrencies remains far off. That said, the resultant legal ambiguity has – surprisingly – benefitted the currency. A deregulated market means few barriers exist for new users and merchants to begin accepting the currency. This is helped through the emergence of several online

---

[110] AFP, 'Bitcoin is Soaring Above $1400 to Another All-Time High' (*fortune.com*, 2 May 2017) <http://fortune.com/2017/05/02/bitcoin-prices/> accessed 5 May 2017.

[111] Alexander Geralis 'Japan Finance Ministry Guides Bitcoin Exchanges, Sets Strict Rules' (*cointelegraph.com*, 3 May 2017) <https://cointelegraph.com/news/japan-finance-ministry-guides-bitcoin-exchanges-sets-strict-rules> accessed 5 May 2017.

[112] 'China Escalates Crackdown on Cryptocurrency Trading' (*Bloomberg.com*, 15 January 2018) <https://www.bloomberg.com/news/articles/2018-01-15/china-is-said-to-escalate-crackdown-on-cryptocurrency-trading> accessed 21 February 2018.

currency exchanges and markets, which have been unhindered in their aim to provide access to Bitcoin to the general public.

The most practical applications of Bitcoin demonstrate the comparative value between decentralised and traditional currencies. For example, sending money internationally becomes significantly cheaper when Bitcoin is used as a platform.[113] Other options, such as credit cards, wire transfers, Paypal (and comparable services), and money transmitters are costly due to the need for an intermediary. For much of the cryptocurrency's history, the peer-to-peer exchanges upon which Bitcoin are based previously cost fractions of a dollar. However, the significant increase in the number of transactions on the Bitcoin network in 2017 resulted in an increase in transaction fees amounting to 18200% in December 2017 when compared to the start of the year.[114] Thereafter, transaction fees dropped and in January 2018 stabilised at approximately double the average cost at the start of 2017. A number of hard forks (eg the Lightning Network)[115] aimed at solving the scalability issues associated with transactions on the network are currently under development, with their ultimate goal being the restoration of Nakamoto's original objective to allow Bitcoin usage for micropayments.

At a more fundamental level, Bitcoin represents a shift in power from the sovereign State to the individual. It serves as a model for effective self-regulation, wherein ease of adoption and ease of forking replaces in-fighting and monopolistic inefficiencies inherent in Ogus' original conception. The ideological and technical foundations of Bitcoin are inherently deregulatory to the extent that Nakamoto coded a veiled criticism of the 2009 German bailout into the blockchain's 'genesis block'.[116]

---

[113] 'Does It Make Sense to Use Bitcoin to Transfer Money to Yourself Internationally?' (*StackExchange*, 24 May 2014) <https://bitcoin.stackexchange.com/questions/25583/does-it-make-sense-to-use-bitcoin-to-transfer-money-to-yourself-internationally> accessed 5 May 2017.

[114] 'Bitcoin Average Transaction Fee Historical Chart' (*BitInfoCharts*) <https://bitinfocharts.com/comparison/bitcoin-transactionfees.html> accessed 21 February 2018.

[115] Joseph Poon and Thaddeus Dryja, 'The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments' (2016) <https://lightning.network/lightning-network-paper.pdf> accessed 21 February 2018.

[116] For an explanation on what a genesis block entails, see 'Genesis Block' (*Bitcoin Wiki*) <https://en.bitcoin.it/wiki/Genesis_block> accessed 5 May 2017.

The key issue that will define the future of Bitcoin is stability. Unlike traditional currencies, Bitcoin's stability does not derive from policy decisions at the State level. Instead, it is directly tied to supply-and-demand, with overall supply being limited in the long run by Nakamoto's algorithm on mining difficulty. Ohnesorge argues that the significant volatility seen in the Bitcoin market in late 2017 hampers the cryptocurrency's ability to act as a medium of exchange and a store-of-value, both of which are key economic functions of a currency.[117] Notably, the shift in usage of Bitcoin from currency to investment has seen several 'traditional' Bitcoin users (eg darkweb merchants) move to Litecoin, Monero, and other altcoins to take payments.[118] This suggests that Bitcoin has lost the key features that made it popular for anonymous transactions online (ie fast speed of payments, stable price, and a low regulatory burden for purchase and sale).[119]

The inherent benefits of cryptocurrencies continue to have lasting appeal beyond the immediate value of each coin at a given time. The demand for a means through which to make digital payments free from government oversight and third-party intermediaries creates a userbase that is inherently 'sticky' and can continue to maintain critical mass beyond market fluctuations. These users form the core of the community, running nodes and mining for Bitcoin through periods of instability. In terms of longevity, it is this userbase that is Bitcoin's best chance for survival.

Whether cryptocurrencies like Bitcoin are little more than a fad or whether they represent a broader shift towards individual empowerment within e-commerce, it is remarkable that an experiment by an anonymous programmer has had this profound impact on our concept of (digital) wealth. It is apt to conclude by noting that Bitcoin has seen exponential growth throughout 2017, despite significant volatility and the late-2017 market crash.[120] Increased mainstream use,

---

[117] Jan Ohnesorge, 'A Primer on Blockchain Technology and Its Potential for Financial Inclusion' (2018) German Development Institute Working Paper, 27 <https://www.die-gdi.de/uploads/media/DP_2.2018.pdf> accessed 21 February 2018.

[118] Andrei Barysevich and Alexandr Solad, 'Litecoin Emerges as Next Dominant Dark Web Currency' (2018) Recorded Future Report CTA-2018-0208 <https://www.recordedfuture.com/dark-web-currency> accessed 21 February 2018.

[119] ibid.

[120] Natalie Sherman, 'It's Not Just Bitcoin Anymore...' *BBC* (London, 24 May 2017) <http://www.bbc.co.uk/news/business-40021902> accessed 24 May 2017.

alongside growing interest amongst commercial investors, has elevated Nakamoto's experiment to the status of *de facto* flagship cryptocurrency. Bitcoin daily trading activity has increased six-fold since 2013,[121] having peaked at upwards of 353,000 confirmed unique transactions in December 2017.

The long-term prospects of the platform remain unclear, with scalability and volatility presenting significant obstacles to Bitcoin's status as a 'legitimate' currency. The rise in competing altcoins (eg Ethereum, Litecash) may also render Bitcoin obsolete, as has been seen among illicit traders. The consensus-building nature of the currency may ultimately give it the long-term adaptability needed to survive, as competing forks optimise the platform over several iterations. Without any form of centralised control over the cryptocurrency, the burden of ensuring Bitcoin's survival falls solely upon its userbase.

[121] 'Confirmed Transactions Per Day' (*Blockchain*) <https://blockchain.info/charts/n-transactions?timespan=all> accessed 21 February 2018.