Journal of Economic Issues

ISSN: 0021-3624 (Print) 1946-326X (Online) Journal homepage: https://www.tandfonline.com/loi/mjei20

Theory and Reality of Cryptocurrency Governance

Antoon Spithoven

To cite this article: Antoon Spithoven (2019) Theory and Reality of Cryptocurrency Governance, Journal of Economic Issues, 53:2, 385-393, DOI: 10.1080/00213624.2019.1594518

To link to this article: https://doi.org/10.1080/00213624.2019.1594518

JOURNAL OF ECONOMIC ISSUES
Volume LIII No. 2 June 2019
DOI 10.1080/00213624.2019.1594518

Theory and Reality of Cryptocurrency Governance

Antoon Spithoven

Abstract: I analyze cryptocurrency ecosystems with Elinor Ostrom's meta-framework for self-governance. I conclude that Bitcoin falls short in its self-governing ambitions, while cryptocurrency software protocols and blockchain technologies have potentialities within "permissioned" peer-to-peer private or hybrid networks. However, regulation and supervision by trusted third parties are required.

Keywords: cryptocurrency, governance

JEL Classification Codes: B52, E4, E5, L5

Satoshi Nakamoto (2008, 1) developed "an electronic payment system based on *cryptographic proof instead of trust* [emphasis added], allowing any two willing parties to transact directly with each other without the need for a trusted third party [. . . Within this system, a] peer-to-peer network timestamps transactions by hashing them" cryptographically into a blockchain. Public blockchains are claimed to prevent cheating and to bypass extractive external institutions (Halpern 2018, 54). As such, the network might be interpreted as a self-governing system. It fits in with the libertarian-inspired Silicon Valley dream that computer networks can create order in society without transaction cost increasing human control.

Several cryptocurrencies (coins and tokens) have been created and disappeared since the launch of the Bitcoin.[1] Coins, such as Bitcoin, are developed as a general medium of

Antoon Spithoven is a research fellow at the Utrecht University School of Economics Research Institute. *The author wishes to thank Hanna Deleanu and Marja Boer for helpful comments.*

[1] On April 25, 2018, there were 1,591 cryptocurrencies (coins and tokens) traded on 10,635 markets (exchanges times currency traded). Until April 10, 2019, 1,027 new currencies (of which 219 are non-mineable) were introduced, and 458 currencies disappeared. The number of markets increased to 17,673, while around 3,500 markets disappeared (https://coinmarket.com). The rise in the number of cryptocurrencies (36%) and markets (66%), indicate respectively a new financing and revenue model, while the number of failing cryptocurrencies (21%) and disappearing markets either reflect a Ponzi scheme or indicate that the public exercises restraint and or that some releases are fraudulent in character. The revenue options increased with the opening of Bitcoin Futures in December 17, 2017. Spoofing might have boosted the prices. The sharp drop in value until February 7, 2018 might indicate a dumping of cryptocurrency by traders.

exchange. Tokens or Initial Coin Offerings (ICOs) appear under the flag of fundraising for development and provision of a specific new service or product.[2] Getting a cryptocurrency accepted is assumed to be subject to the market mechanism. However, the fact remains that one must convince the public that programmers will deliver what is promised and that the cryptocurrency will have value.

Elinor Ostrom's (2005) Institutional Analysis and Development (IAD) model for self-governance provides handles to answer the question if the cryptocurrency consensus algorithm is a sufficient substitute for trust in a peer-to-peer electronic payment system (Smith and Crown 2016).[3] Though self-governance may suggest a libertarian disposition, Ostrom was not a libertarian or a supporter of a stateless society.[4]

Self-Governing Systems

Ostrom (2005, 99, 103) assumed individuals to be basic units of decision-making. Her game-theoretic analyses are based on assumptions concerning: (1) acquired partial or complete information, its asymmetric or symmetric distribution, and its imperfect or perfect processing; (2) valuation processes (rational egoism, trust, or reciprocity), and; (3) processes of selection (maximizing, satisficing, or using diverse rules of thumb).

Ostrom (1992, 67–79; 2005, 59, 259) integrated eight self-governance conditions in the IAD model to analyze governing the commons as a more efficient governance structure than markets and governments. These self-governance conditions concern: clearly defined boundaries (objectives) and memberships, proportional incentives, actively auditing monitors, collective choice arrangements, graduated sanctions, conflict resolution mechanisms, rights that are recognized by "external governmental authorities," and nested local rules within governmental rules at regional and national levels. I analyze cryptocurrency ecosystems in view of the first three conditions.

Cryptocurrency Ecosystems

Cryptocurrency ecosystems may include: the initiators, the codebase, programmers, miners, middlemen, customers, the media, and governments.[5] See Figure 1.

Initiators of Cryptocurrency and Internet Platforms

The sales pitch of cryptocurrency organizations is that "money supply should not be used as an instrument of monetary policy as inflation destroys value and encourages

[2] The ICOs "can be traded for services, once the business is operational—whenever that is—or traded for crypto- and other currencies" (Halpern 2018, 56).

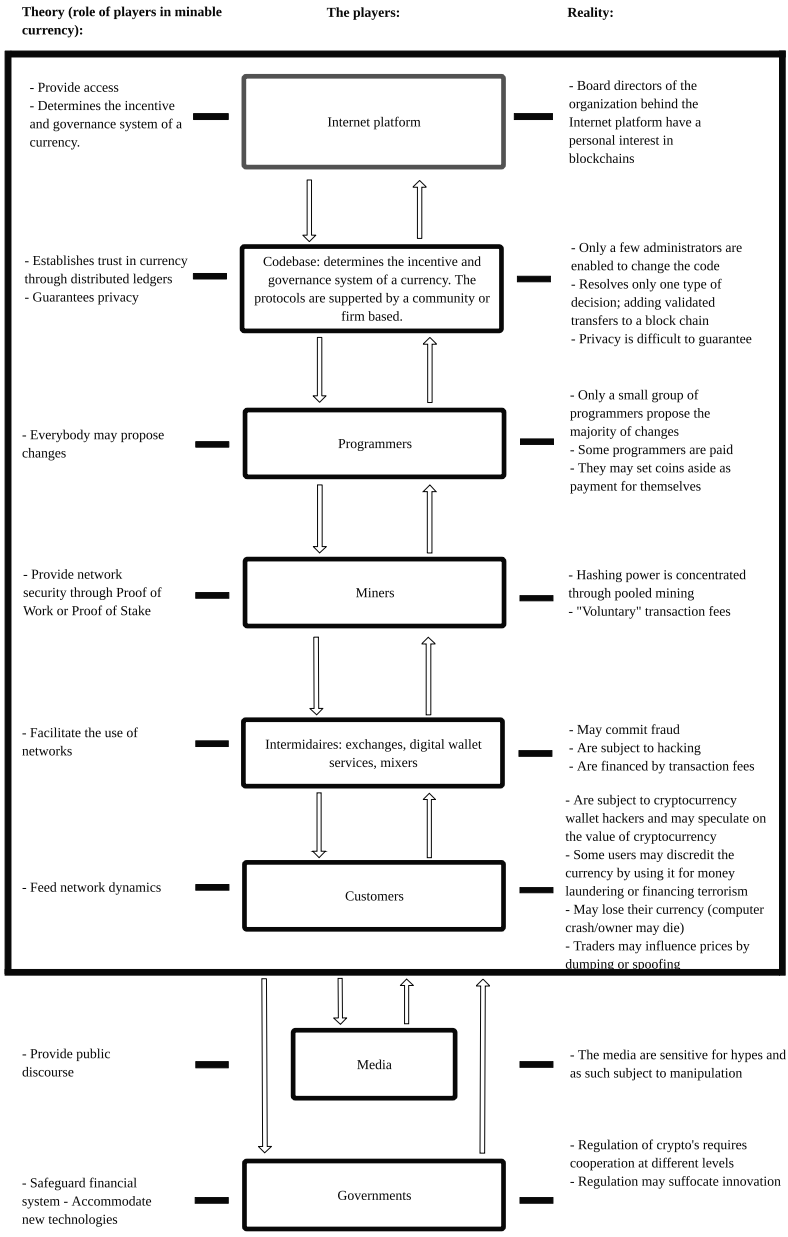
[3] Ostrom (1992) elaborated her model for analyzing self-governance of non-tradeable resources. The model might be extended to tradeable goods as well.

[4] First, Ostrom (2005, 24) claims that commons represent not private but common-pool resources. Second, commons are one of many possible efficient governance structures. She (2005, 249, 268) allows governmental authorities to step in.

[5] Due to limited space, I focus on differences between theory and practice, while differences in practice (see Hileman and Rauchs 2017) cannot be dealt with.

unsustainable consumption" (Bitcoin Foundation 2018b). Therefore, governments should have to become disabled to smooth business cycles and this can be achieved by setting supply at a final limit or allowing for a steady increase.

Figure 1. The Ecosystem of Minable Currency



Source: adapted from Smith and Crown (2016)

Organizations behind cryptocurrency influence their governance. For example, the Bitcoin Foundation (2018a, 2018b, 2018c)—whose directors have a personal interest in blockchains—and other non-profit organizations coordinate efforts of cryptocurrency communities such as funding of core programmers, lobbying upon legislators to make cryptocurrency a success, and developing a platform. Values expressed by the Bitcoin Foundation concern privacy, guaranteed financial access, decentralization ("centralization of money supply leads to corruption and exploitation"), autonomy, financial inclusion, and stable money supply.

Cryptocurrency internet platforms (such as bitcoin.org) are owned by the community but are likely to be influenced by sponsors (for instance, the exchange Paxful) and the website maintainer. The platforms give customers and providers of services access to public ledgers. Customers are consumers and businesses (such as, traders). Providers of processing services are programmers and validators of transactions (the so-called miners). Providers of financial services are middlemen such as wallet providers, exchanges, and mixers. Mixers lump transactions together to obfuscate the identity of customers.

Cryptocurrency are Rooted in a Code

The software behind the Bitcoin payment system is common. The open-source license enables everyone to propose changes to the software, while trust is assumed to be established through decentralized public ledgers in the form of a blockchain: a system to share information and to store the history of transactions on a computer network (Halpern 2018, 54). The blockchain is assumed to foster efficiency by lowering transaction cost through consensus algorithms, minimizing counterparty risk, reducing settlement times, eliminating unnecessary middlemen, improving contractual term performance, improving regulatory control, and increasing transparency for regulatory reporting.

The basic code of a public ledger encloses: the rules for transactions (protocol for sending, receiving, and recording value using cryptographic methods), hash protocols (linear or tree-based protocols), block attributes (block version number, timestamp, hashes—that is, input strings of any length are transformed in output strings of a fixed length), and consensus mechanisms. To determine which blockchain is valid there are two coordination rules: first the longest blockchain is generally assumed to be reliable, and second, checkpointing—that is, a mined block must be linked (not to genesis one but) to a more recent blockchain (Abramowicz 2016, 374–375).

The Bitcoin protocol serves several functions. The protocol provides a financial reward to miners "for generating a block of transactions to add to the end of the block chain [. . . Besides, they may] receive transaction fees from transferors of bitcoins, who voluntarily include these fees in their transactions to encourage miners to include the transactions in a block" (Abramowicz 2016, 376). Transactions are by design irreversible, even if a contract is incomplete. Another function of the Bitcoin protocol concerns one's privacy. Customers are not required to register one's real identity.

In fact, the codebase is constantly evolving (new tools, functions and services are developed to improve security and acceptance), might become hacked, and may result in hard *forks*. Forking indicates "inconsistencies in the replicas in the network" (Decker and Wattenhofer 2013, 1; Abramowicz 2016, 372), and might be harmful for the relevant cryptocurrency (Gervais et al. 2014). Inconsistencies "facilitate an attacker that attempts to

rewrite transaction history" and may undermine trust in the cryptocurrency (Decker and Wattenhofer 2013, 1). A no-forking guarantee requires a patented codebase rather than an open source codebase.

Programmers

The bitcoin programmers centrally coordinate the Bitcoin protocol (Abramowicz 2016, 367). They regulate the Bitcoin through their decisions regarding forking and blocking interactions from specific addresses (coin tainting) (Gervais et al. 2014). Some forks might be malicious and serve the financial interests of programmers who set aside a certain amount of coins as payment for themselves.

Core programmers of the source code may benefit from volunteers by making the software available freely to everyone. Regarding the Bitcoin there is a concentration of programmers who contribute to the codebase and a concentration of commenters who propose changes to the codebase (Azouvi, Maller, and Meiklejohn 2018). It may result in different versions of the coin involved.[6]

Miners

An electronic payment network such as Bitcoin is an institution that "creates and enforces property rights [. . . , and] that can resolve only one type of decision-making: whether purported transfers [. . .] will be validated and added to [. . .] the block chain" (Abramowicz 2016, 361). Labor of miners is involved to verify legitimacy of transactions. They are rewarded with coins "for their services in addition to possible [. . .] transaction fees" (Evans 2014, 12).

Miners provide network security through either Proof of Work (PoW) or Proof of Stake (PoS) (Rosic 2017; Halpern 2018, 54). The difference between PoW and PoS concerns who creates a new block. In a PoW system, a new block is created by the miner who is the first to solve the math problem that is involved in creating a new block. In a PoS system, the miner who has the most coins can create a new block. The PoW requires high investments (large-scale operations), is time consuming, and energy inefficient. It increases the risks of engaging in the form of mining in which payments are awarded randomly. Pools of miners emerged to diversify random payment risks (Evans 2014, 18). Miners may join the pool and might be charged a membership fee. Some pools disclose and share transaction fees. The PoS is subject to monopolization by means of organizations with big stakes (owners of a large share in the volume of available coins).

A colluding power block of miners may "effectively control [the confirmation of] all transactions, for example, preventing certain transactions' execution, approving a specific set of transactions [among which, adding blank blocks to the blockchain], or approving double-spending transactions" (Gervais et al. 2014, 55). The pool also prescribes the type of

[6] There exists about forty variants of the Bitcoin (https://coinmarketcap.com/), most of them have a maximum supply of 21 million coins. Bitcoin Gold (5% is set aside as a bonus), Bitcoin Cash, and Bitcoin Silver are three examples of a hard fork of the Bitcoin. Namecoin and Litecoin are based on the Bitcoin technology, while Dogecoin is a fork of Litecoin (Evans 2014, 16).

protocol that your computer follows. Finally, a power block of more than fifty percent may create a new hard fork (Gruber 2013, 163).

Middlemen: Wallets, Exchanges, Mixers

Cryptocurrencies require a whole set of intermediaries in the form of firms that provide processing and financial services. Ironically, the criticized banking system is also involved: traders use virtual stablecoins (for example, Tether, TrueUSD, PAX, AUD (Australian dollar)), which are pegged to fiat currency or gold, for trading cryptocurrency on exchanges. According to Rainer Böhme et al. (2015, 222), there are several problems with middlemen: currency exchanges may fail; digital wallet providers may steal cryptocurrency; mixing "protocols are usually not public" which enables mixers, who disconnect originating and receiving addresses, to run away with funds; all middlemen charge commissions or fees, and; consumers and heirs-at-law may lose coins (because of crashed/hacked computers respectively decease). Additionally, Böhme et al. (2015, 226) mention: trade in large amounts (in the form of dumping or spoofing) influence the price of the currency; closing of exchanges; "and legal and regulatory risk."

Customers

Customers feed the network dynamics. Their transactions, behaviors, and risks to which they are exposed result in adopting, rejecting, adapting, or even hard forking of cryptocurrency. Among other things, the volatility of coin value did prevent cryptocurrencies from becoming a general-purpose currency as proclaimed (Irwin 2018).

The value of coins fluctuates because expectations over demand are influenced by a myriad of factors. Examples of these factors are: there is no third party to intervene to stabilize the value, new cryptocurrency or disappearing cryptocurrency may influence the price of other currency, and customers of cryptocurrency are multiple in kind. Demand for a specific cryptocurrency may rise because customers may use cryptocurrency not only for lawful transactions, but also for tax evasion, money laundering, extortion, prostitution, human trafficking, speculation, and trade in drugs and weapons (Gruber 2013).

Other reasons that cryptocurrencies are ill-suited as a medium of exchange or as a reliable unit of account, are: transaction risks (bankruptcies of financial service providers, difficult to use), uncompetitive applications (low transaction speed, delay of verification), operational risk (operator errors, malware, security flaws, platform lock-in of programmers), privacy-related risk (Evans 2014), and high fees.

Additionally, privacy is, after all, difficult to guarantee. One's identity might become revealed through one's delivery address for a purchase of a commodity (Böhme et al. 2015, 221), and through one's cryptocurrency-exchange account (Liedel 2018, 113). To stay under the radar customers may use the automatically changed wallet address after each transaction. They also may use software providing anonymity like Tor, or, in exchange of a fee, they may call in poolers of transactions (Böhme et al. 2015).

The Media

The media have the power to enable public discourse, to redirect the public discussion on pros and cons of cryptocurrency, and to influence the price. Investigative journalism might provide customers and service providers with critical information regarding potentialities of new technologies, the misuse of these technologies, and existing or lacking regulations. However, (social) media are subject to hype, fake news, and news on money laundering, speculation, and manipulation by traders. This might disable their monitoring and information function. Their focus on irregularities may distract the public from potentialities of the blockchain technology (Papadopoulos 2015, 128).

Governments

Cryptocurrency adherents believe that public ledgers make regulating and supervising by (extractive) agencies obsolete. Their claim is misplaced because blockchain technology concerns only registering and validation of a transaction. Participants of cryptocurrency ecosystems are unable to monitor and sanction misbehaviors. According to Sarah Gruber (2013, 162), "the Bitcoin ecosystem is far less trustworthy than the banks that the Bitcoin proponents denounce as untrustworthy."

Cryptocurrencies and their blockchain technology have gained so much popularity that governments cannot simply forbid them. At the risk of suffocating innovation and the chance to boost innovation by legitimizing it (Hughes and Middlebrook 2015, 499), the use of cryptocurrencies and the supply of services based on cryptocurrencies should become regulated and supervised for the sake of fighting crime, protection of traditional infrastructures, and protection of consumers. Additionally, regulation and supervision are also desired to safeguard the financial system. Namely, the traditional financial system is challenged by cryptocurrency. Cryptocurrency may "transform the monetary system as a whole" (Papadopoulos 2015, 128).

To integrate public ledgers in properly operating markets, blockchain technologies must be nested in a whole set of institutions which not only addresses rights, duties, liberties, and exposures of all parties involved, but also enable monitoring, sanctioning, and conflict resolution. Regulation of intermediaries to cryptocurrency transactions might become inspired by "regulations governing existing payment mechanisms" so that cryptocurrency transactions might become recorded, verified, and monitored (Hughes and Middlebrook 2015, 498, 513).

Prudential and market regulation of cryptocurrency are still in their infancy. Existing regulation of cryptocurrencies concentrates on public purposes, among which are tax collection and fighting criminal activities and monetary losses. Governmental authorities focus especially on regulating cryptocurrency middlemen (Hughes 2017, 21). Examples of these types of regulations are: (1) the requirement in the United States of America to register with the Financial Crimes Enforcement Network, or; (2) the requirement to register with the Commodity Futures Trading Commission, and; (3) the reporting requirements of the Bank Security Act for "money transmission services [. . . including] substitutes for currency" (Gruber 2013, 173). However, federal regulations are not specified to cryptocurrency, "which makes enforcement of any new legal framework tenuous" (Hughes 2017, 1).

Cryptocurrency lacks default rules that "apply in the absence of negotiated contracts or when negotiated contracts are silent on the issue in question" (Hughes and Middlebrook 2015, 502, 507, 549; Tu 2018, 538–539). Codification might be based on assessing existing practices such as Bitlicense in New York (Claasen 2017). Some of existing regulations of traditional currencies might be extended to cryptocurrencies. For example, the Internal Revenue Service approaches cryptocurrency as property—which allows capital gains and the value of the property to be taxed—but might reconsider cryptocurrency as a currency (Liedel 2018) or as collateral (Tu 2018).

The public blockchain technology is an example of innovation that the framers could never have foreseen. Blockchain technology is thought to enable a reliable and decentralized record keeping of "virtually everything of value" (Liedel 2018, 110).[7] It challenges traditional property rights: blockchain ownership is shared ownership, while blockchain technology enables one to issue, own and manage digital assets. It creates a new pitch that may transform the concept of ethical business or corporate social responsibility. It might become federally regulated in accordance with the Commerce Clause by relaxing the interpretation of the Commerce Clause (Kennedy 1995, 6, 13).

In addition to regionally regulating cryptocurrencies, governments should also cooperate internationally to combat the misuse of cryptocurrency, and to protect the cryptocurrency features, because customers that transfer cryptocurrency "may fall outside the regulatory scope" of a nation's law, or because exchanges may move "to countries with less regulation." Probably governments must also prohibit mixing services and the Tor network (Gruber 2013, 139–140, 189,193).

Conclusion and Discussion

The application of Ostrom's criteria for self-governance shows that cryptocurrency requires more than computer algorithms. Hashing power is concentrated in mining pools. Providers of processing services are more concentrated and less transparent than the Bitcoin-design suggests. Providers of financial services are subject to several failures. Multifarious users may game cryptocurrency ecosystems to (illegally) reap benefits. Although organizations behind peer-to-peer networks may enforce improvements on incentives and governance, regulation and supervision by external institutions are desired. Without strong external regulation, cryptocurrency may resemble Veblenian (predatory) markets.

Although blockchain technology does not yet deliver what is suggested with its application in cryptocurrency, it is nevertheless promising. It might be used to register all kinds of transactions, save on transaction costs, and stimulate innovation. Vested interests may turn to permissioned private blockchains—that is, blockchains for clearly defined objectives and memberships, for example, firms—or to hybrid blockchains (consortia).

It will take a long time before blockchain is going to fundamentally influence society and economy. As is known from the institutional literature, new technologies may incite resistance. Additionally, governments need time to develop laws that legitimize and

[7] The blockchain, whether or not adapted for invitation-only peer-to-peer networks, could be used to facilitate transactions of several kinds of digitized data, such as property. Also, smart "contracts could be written and stored on the blockchain." A smart contract might be a loan: "I send you some money, and your account automatically pays it back, with interest" (Halpern 2018, 54, 56). The task performance might change of notaries, lawyers, auditors, administrators, and arbitrators who are involved in agreeing, controlling, and enforcing contracts.

constrain application of blockchain technology. Furthermore, regulation is a devil of a job: different levels of government should cooperate and fit international agreements to local circumstances. Finally, given appropriate cultural conditions, the time needed to familiarize and to adapt oneself to technologies is determined by their *novelty* and *complexity* (use, reach, process-substitution and system-transformation) (Iansiti and Lakhani 2017; my emphasis).

References

Abramowicz, Michael. 2016. "Cryptocurrency-Based Law." *Arizona Law Review* 58 (359): 359–420.

Azouvi, Sarah, Mary Maller, and Sarah Meiklejohn. 2018. "Egalitarian Society or Benevolent Dictatorship: The State of Cryptocurrency Governance." The Fifth Workshop on Bitcoin and Blockchain Research, https://fc18.ifca.ai/bitcoin/papers/bitcoin18-final13.pdf. Accessed May 30, 2018.

Bitcoin Foundation. 2018a. "Board of Directors." bitcoinfoundation.org. Accessed May 17, 2018.

Bitcoin Foundation. 2018b. Homepage. bitcoinfoundation.org. Accessed May 17, 2018.

Bitcoin Foundation. 2018c."The Bitcoin Foundation Manifesto." bitcoinfoundation.org. Accessed May 17, 2018.

Böhme, Rainer, Nicolas Christin, Benjamin Edelman, and Tyler Moore. 2015. "Bitcoin: Economics, Technology, and Governance." *Journal of Economic Perspectives* 29 (2): 213–238.

Claasen, Llew. 2017. Letter from the Executive Director of the Bitcoin Foundation to The National Conference of Commissioners on Uniform State Laws, July 14, 2017, http://www.uniformlaws.org. Accessed June 12, 2018.

Decker, Christian and Roger Wattenhofer. 2013. "Information Propagation in the Bitcoin Network." Thirteenth IEEE International Conference on Peer-to-Peer Computing.

Evans, David S. 2014. "Economic Aspects of Bitcoin and Other Decentralized Public-Ledger Currency Platforms." *Working Paper No. 685 (2nd series)*, Coase-Sandor Institute for Law and Economics, University of Chicago, April 2014.

Gervais, Arthur, Ghassan O. Karame, Srdjan Capkun, and Vedran Capcun. 2014. "Is Bitcoin a Decentralized Currency?" *IEE Security & Privacy* 12 (3): 54–60.

Gruber, Sarah. 2013. Exchanges the Next Virtual Havens for Money Laundering and Tax Evasion." *Quinnipiac Law Review* 32 (1): 135–208.

Halpern, Sue. 2018. "Bitcoin Mania." *The New York Review of Books* 65 (1): 52, 54, 56.

Hileman, Garrick and Michel Rauchs. 2017. *Global Cryptocurrency Benchmarking Study*. Cambridge: University of Cambridge, Judge Business School.

Hughes, Sarah Jane and Stephen T. Middlebrook. 2015. "Advancing a Framework for Regulating Cryptocurrency Payments Intermediaries." *Yale Journal on Regulation* 32 (2): 495–559.

Hughes, Scott D. 2017. "Cryptocurrency Regulations and Enforcement in the U.S." *Western State University Law Review* 45 (1): 1–28.

Iansiti, Marco and Karim R. Lakhani. 2017. "The Truth About Blockchain." *Harvard Business Review* 95 (1): 118–127.

Irwin, Neil. 2018. "Should the Fed Create "FedCoin" to Rival Bitcoin?" *The New York Times,* May 4, 2018.

Kennedy, Anthony McLeod. 1995. [Concurring Opinion] *United States v. Alfonso Lopez*, doc. No. 93-1260. Supreme Court of the United States, April 26, 1995.

Liedel, Deidre A. 2018."The Taxation of Bitcoin: How the IRS Views Cryptocurrencies." *Drake Law Review* 66 (1): 107–145.

Nakamoto, Satoshi 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System." (October 31, 2008). http://nakamotoinstitute.org/bitcoin/. Accessed May 7, 2018.

Ostrom, Elinor. 1992. *Crafting Institutions; Self-Governing Irrigation Systems*. San Francisco, CA: Institute for Contemporary Studies Press.

Ostrom, Elinor. 2005. *Understanding Institutional Diversity*. Princeton and Oxford: Princeton University Press.

Papadopoulos, Georgios. 2015. "Expanding on Ceremonial Encapsulation: The Case of Financial Innovation." *Journal of Economic Issues* 49 (1): 127–142.

Rosic, Ameer. 2017. "What is Hashing? Under the Hood of Blockchain." August 2017, https://blockgeeks.com/guides/what-is-hashing/, Accessed May 17, 2018.

Smith and Crown (Research organization). 2016. "Intro: Cryptocurrency Governance (of, by, for the users?)." March 24, 2016, https://www.smithandcrown.com. Accessed May 30, 2018.

Tu, Kevin V. 2018. "Perfecting Bitcoin." *Georgia Law Review* 52, no. 2 (Winter): 505–580.