McGill Law Journal — Revue de droit de McGill

TAX *CRYPTOGRAPHIA*: EXPLORING THE FISCAL DESIGN OF CRYPTOCURRENCIES

*Allison Christians**

While the founders of cryptocurrencies may not conceptualize their efforts as such, the infrastructural choices they make in designing their systems mimic those routinely made by lawmakers in the design of fiscal policy. The totality of their decision-making in this regard constitutes essential elements of "taxation" written into the governance structure of the cryptocurrency system — its tax *cryptographia*. This article examines how cryptocurrency founders determine what common goods are necessary to make their systems viable and then design a way to fund them. The object of comparing certain cryptographic design elements to taxation is to examine how investors, speculators, enthusiasts, and skeptics should assess the decisions that founders make, and why it might matter if the participants in cryptocurrency systems recognize the fiscal infrastructure as a reproduction of state-like functions that serve to allocate the cost and benefits of participating in the collective activity despite the core motivation of cryptocurrency to bypass centralized and hierarchical political institutions.

Si les fondateurs des cryptomonnaies ne conceptualisent pas nécessairement leurs efforts en ce sens, les choix infrastructurels qu'ils font dans la conception de leurs systèmes imitent ceux que font couramment les législateurs dans la conception des politiques fiscales. L'ensemble de leurs décisions à cet égard constitue des éléments essentiels de la « fiscalité » inscrits dans la structure de gouvernance du système des cryptomonnaies — sa cryptographia fiscale. Cet article examine comment les fondateurs des cryptomonnaies déterminent les biens communs nécessaires pour rendre leurs systèmes viables et conçoivent ensuite un moyen de les financer. Le but de comparer certains éléments de conception cryptographique avec la fiscalité est d'examiner comment les investisseurs, les spéculateurs, les amateurs et les sceptiques devraient évaluer les décisions que prennent les fondateurs, et pourquoi il pourrait être important que les participants aux systèmes de cryptomonnaies reconnaissent l'infrastructure fiscale comme une reproduction des fonctions de type étatique qui servent à répartir les coûts et les bénéfices de la participation à l'activité collective, malgré la motivation fondamentale des cryptomonnaies, qui n'est autre que de contourner les institutions politiques centralisées et hiérarchisées.

* Allison Christians, H. Heward Stikeman Chair in the Law of Taxation, McGill University Faculty of Law. Thanks for comments on early drafts go to Kim Brooks, Ignacio Cofone, Rumi Guzdow, Max Jarvie, Shuyi Oei, Marc Richardson, Diane Ring, Oleg Stratiev, the participants of the McGill Law Journal symposium Programming Governance/Governing Programming: Regulatory Challenges on the Edge of Technology, and two anonymous reviewers.

Citation: (2019) 64:4 McGill LJ 683 — Référence : (2019) 64:4 RD McGill 683

Introduction 685

I. Background: Fiscal Infrastructure Elements 687
A. *The Infrastructural Core: Decentralized Ledger Technology* 688
B. *Block Production Reward Design* 689
C. *Transaction Fee Design* 690
D. *System Sustainability* 691

II. Blockchain's Fiscal Logic: Is It Taxation? 693
A. *Mining is Obligatory* 694
B. *Mining Produces a Quasi-Public Good* 696
C. *Tax Cryptographia Emerges* 698

III. A Policy Assessment of Tax Cryptographia 699
A. *Often Inflationary, Inherently Regressive* 700
B. *Tax Cryptographia is Inevitable* 702

Conclusion 704

Introduction

When Bitcoin launched in 2008, cryptocurrency enthusiasts viewed it as a major disruptor of government power because it provided an alternative to government-controlled currency.[1] To those who view government largely as an encumbrance, this new technology promised to bypass centralized and hierarchical political institutions using distributed consensus, laying the foundation for an idealistic society of equals.[2]

The act of decentralizing away from the state is often associated with an increase in personal freedom from the power of the collective.[3] The argument put forward by early cryptocurrency enthusiasts was that personal freedom would be increased if individuals were given full use of their own economic resources, free of any form of coercive taxation towards collective purposes.[4] But some of the core design elements of cryptocurrencies demonstrate that all communities—even virtual ones—inevitably find it necessary to pool resources to produce goods used by all. Even in the world of cryptography, the sphere of personal freedom over one's own resources is limited by the need to sustain the community in which one operates.

An inspection of the fiscal design of popular cryptocurrencies demonstrates that their founders inevitably develop a core set of governance goods, comparable to public goods developed by states. These goods are in-

---

1 See Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Cash System" (2009), online (pdf): *Bitcoin* <www.bitcoin.org/bitcoin.pdf> [perma.cc/2AJP-RA4R] (launching the idea of Bitcoin); Alan Feuer, "The Bitcoin Ideology", *New York Times* (14 December 2013), online: <www.nytimes.com> [perma.cc/DK63-7XUQ] ("[a]t first, almost everyone who got involved did so for philosophical reasons. We saw bitcoin as a great idea, as a way to separate money from the state"). The term cryptocurrency as used herein refers to digital currencies that are created, managed, and exchanged using cryptographic protocols. For a more detailed description, see e.g. US, Congressional Research Service Report for Congress, *Cryptocurrency: The Economics of Money and Selected Policy Issues* (R45427) (Washington, DC: Library of Congress, Congressional Research Service, 2018) [CRS Report].

2 See Gilles Paquet & Christopher Wilson, "Governance Failure and Antigovernment Phenomena" (2015) 45:2 Optimum Online 1 at 18–20.

3 See Charlie Shrem, "Bitcoin's White Paper Gave Us Liberty – Let's Not Give It Back", *coindesk* (20 October 2018), online: <coindesk.com> [perma.cc/L3Q4-VYJQ]. Shrem is a convicted felon who served one year in federal prison for operating an unlicensed money-transmitting business, failing to disclose suspicious banking activity, and money laundering: see Shawn M Carter, "What a 20-something Bitcoin Millionaire Learned From Going to Prison and Starting Over", *CNBC* (8 December 2017), online: <www.cnbc.com> [perma.cc/JPY9-7VJK].

4 See e.g. Feuer, *supra* note 1 (explaining that Nakamoto's white paper "attracted followers among libertarian and anarchist groups who saw in bitcoin a means of removing the money supply from the grasping hands of government").

frastructural in nature and essential to the functioning and value of the cryptocurrency. Like governments, cryptocurrency founders must make their foundational infrastructure reliable so that investors and users will continuously contribute to and benefit from the collective value of the community they thereby create. In concrete terms, this means that the founders need to figure out a way to finance the necessary human resources and capital investments to maintain the cryptocurrency over the long term, using resources contributed or generated by developers, miners, investors, and users.

The act of creating a self-sustaining financial structure for a cryptocurrency system looks similar to the act of creating a tax system in several respects. First, creating such a structure obliges the founders to choose how to distribute all currently foreseeable infrastructure costs as well as the potential risks of unknown future costs amongst the various identified stakeholders of the system. The task of identifying such stakeholders is itself a choice similar to what lawmakers face in determining who should be considered a taxpayer. Founders necessarily make these identification and distributional choices with a view not only to providing cryptocurrency holders and users with a given service, just as a business making supply chain cost and quality decisions might do, but also to ensuring the ongoing viability of the underlying structure itself. Further, making these policy choices has economic impacts on individual users and on the system as a whole, akin to the micro- and macro-economic effects of fiscal policy choices within states.

While the founders of cryptocurrencies may not conceptualize their efforts as such, these kinds of infrastructural choices mimic those routinely made by governments in the design of fiscal policy. The intrinsic purpose of fiscal policy is to distribute burdens and benefits among a given populace in order to achieve common goals.[5] In making private order fiscal policy choices, cryptocurrency founders thus confront both individual and system-wide risks and impacts. The totality of their decision making in this regard constitutes essential elements of "taxation" written into the governance structure of the cryptocurrency system—its tax *cryptographia*.[6]

---

5 See generally Allison Christians, "Drawing the Boundaries of Tax Justice" in Kim Brooks, ed, *The Quest for Tax Reform Continues: The Royal Commission on Taxation Fifty Years Later* (Toronto: Carswell, 2013) 53 [Christians, "Drawing the Boundaries"].

6 See Aaron Wright & Primavera De Filippi, "Decentralized Blockchain Technology and the Rise of Lex Cryptographia" (2015), online: SSRN <papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664> (using the term to describe the phenomenon of "rules administered through self-executing smart contracts and decentralized (autonomous) organizations" at 4).

As a representation of the fiscal policy choices of its founders, the tax *cryptographia* of a given cryptocurrency system demonstrates that embedding some mechanism for resource pooling and spending is unavoidable. The emergence of a function that parallels state-based taxation in an endeavour expressly designed (to some, at least) to escape the state and its ubiquitous taxing power is intrinsically fascinating. More fundamentally, the inevitability of tax *cryptographia* offers an opportunity to re-examine why it is that taxation is a fundamentally necessary aspect of any cooperative socio-economic order, even when the underlying rationale in the cryptocurrency sphere is to eliminate the state.

Accordingly, this article examines how cryptocurrency founders determine what basic goods are necessary to make their systems viable and then design a way to fund them. The object is to examine how investors, speculators, enthusiasts, and skeptics should assess the decisions that founders make, and why it might matter if the participants in cryptocurrency systems recognize the fiscal infrastructure as a reproduction of state-like functions that allocate the costs and benefits of participating in the collective activity.

Part I undertakes a brief background of cryptocurrency systems, with a particular focus on their main fiscal elements. Part II analyzes why and how these fiscal elements might be considered a form of, or at least comparable in fundamental ways to, taxation. Part III assesses the choices made by cryptocurrency founders to date and queries how they ought to be assessed. The article concludes that despite the ideological roots of today's cryptocurrencies, it is not possible to design any kind of cooperative social order without fiscal policy. Whether cryptocurrency founders will learn any lessons from the history of taxation is another question.

I. Background: Fiscal Infrastructure Elements

A thorough explanation of the technological innovation behind cryptocurrency is beyond the scope of the current discussion and readily available elsewhere,[7] but a simplified explanation of the general idea of decentralized ledger technology is useful in considering the theory presented in this paper, namely that cryptocurrency founders and developers are engaged in making fiscal choices that mimic taxation and state-building in fundamentally important ways. If this assessment is correct, it tells us something about the nature of cooperative market-making without the state, namely, that effective cooperation cannot be accomplished without

---

[7] For a brief explanation of Bitcoin, see Nathaniel Popper, "What is Bitcoin, and How Does it Work?", *New York Times* (1 October 2017), online: <www.nytimes.com> [perma.cc/P3KH-BLBX].

coercively allocating costs and benefits among participants, and that therefore making sound fiscal choices should be viewed as imperative to designing a viable cryptocurrency. This Part provides a brief overview of various aspects of decentralized ledger-based cryptographic protocol design and maintenance relevant to resource allocation questions, examining the fiscal features of cryptocurrency systems and contextualizing the discussion within the language of taxation.

A. The Infrastructural Core: Decentralized ledger technology

In general, cryptocurrencies modeled after Bitcoin are digital assets produced and traded via a decentralized database that is maintained by a distributed network of computers. Participating computers iteratively record (in "blocks") the history of all the transactions on the network, thus the database is decentralized in the sense that each node stores up-to-date copies of the ledger, thus collectively ensuring the validity of each transaction.[8] Participants who want information added to the blockchain, for example regarding a transfer of an amount of cryptocurrency from one participant's digital wallet to another, must apply to have their transfer recognized by block producers ("miners") who generally receive rewards for their maintenance of the system and for verifying transactions in the form of newly issued cryptocurrency or tokens, in addition to transaction fees provided in respect of each transaction.[9]

---

[8] See Nakamoto, *supra* note 1 ("[w]e define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership" at 2).

[9] Miners receive such fees in "proof of work"-based verification systems: see José Eduardo de A Sousa et al, "An Analysis of the Fees and Pending Time Correlation in Ethereum" (Paper delivered at the 9th Latin American Network Operations and Management Symposium, Brazil, 25–27 September 2019) [unpublished] ("[t]he security of the blockchain is established by a chain of cryptographic puzzles, solved by participants called miners, which are connected by a peer to peer network. The miner that first solves a crypto puzzle can record a block of transactions, and then receive a fee from users as a reward for its mining (computational and power) effort, also known as proof of work" at 1). See also Arvind Narayanan et al, *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction* (Princeton: Princeton University Press, 2016) at 136; Adam S Hayes, "Cryptocurrency Value Formation: An Empirical Analysis Leading to a Cost of Production Model for Valuing Bitcoin" (2017) 34:7 Telematics & Informatics 1308 ("[n]ew bitcoins are created as a reward for transaction processing work in which users offer their computing power to verify and record payments into the public ledger. Also known as 'mining', individuals or firms engage in this activity in exchange for the chance to earn newly created blocks of bitcoins" at 1309). Proof of work is not the only possible cryptographic validation system; proof of stake validation may ultimately replace mining, with alternate consequences: see e.g. Iddo Bentov et al, "Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake" (2014) 45:2

In the Bitcoin blockchain, miners initially received fifty Bitcoin for mining a new block. The Bitcoin protocol provided for the reward to be halved every 210,000 blocks, which is approximately every four years.[10] At the time of writing, the reward is twelve and a half Bitcoin per new block.[11]

The compensation of miners can be characterized as a fiscal design choice in the sense that it is a systemic and unavoidable cost added to all private transactions, it is undertaken for communitarian reasons, and it has distributional economic impact. The cost to compensate the essential block production, which is collectively a blockchain maintenance function, may be characterized as quasi-private (transaction fees) or quasi-public (block rewards) in nature, as described below.

B. Block Production Reward Design

The security, certainty, and decentralization of cryptocurrency systems do not occur as natural features but require time and resource investment. In particular, cryptocurrencies depend on constant updating in the form of block production. Block production rewards may be viewed as a quasi-public component of cryptocurrency fiscal design because they are paid out by issuing new tokens—that is, printing money. The issuance of new currency alters the outstanding supply and therefore affects all those in the network, whether they are actively transacting in the currency or not.

The amount of rewards paid to block producers may change over time either by predetermined schedule, as described above in the case of Bitcoin, or by community consensus. For example, Ethereum rewards are periodically set at a specified number per block according to analysis and consensus of the mining community.[12]

Accordingly, with each block produced, wealth is effectively transferred from all existing token holders to the block producers in the form of

---

Performance Evaluation Review 34; Shuyang Tang & Sherman SM Chow, "Systematic Market Control of Cryptocurrency Inflations" (2018) Association for Computing Machinery Working Paper Session No 3.

10 See "Bitcoin Block Reward Halving Countdown" (10 December 2019), online: *Bitcoin Block Reward Halving Countdown* <www.bitcoinblockhalf.com> [perma.cc/SG3D-23R5] ["Halving Countdown"]; Joseph Young, "Will the Upcoming Mining Reward Halving Impact Bitcoin's Price?" *Bitcoin Magazine* (10 February 2016), online: <bitcoinmagazine.com> [perma.cc/HD4Y-AGTF].

11 See "Halving Countdown", *supra* note 10.

12 See e.g. Eric Conner, "A Case for Ethereum Block Reward Reduction to 2 ETH in Constantinople (EIP-1234)" (27 July 2018), online: *Medium* <medium.com/@eric.conner> [perma.cc/7FM5-GLF4].

inflation. The extent of the inflation produced by rewarding miners might be relatively modest. In the case of Bitcoin, for example, the estimate is currently 3.7 per cent per year, which is expected to drop to 1.8 per cent per year after the next reward-halving event occurs.[13] For non-finite cryptocurrency models, it is harder to determine the effect of new currency issuance for block production. Miners may be expected to trade on their relative sophistication regarding expected inflationary profits.[14]

Where the available amount of the cryptocurrency to be produced is finite, as it is in the case of Bitcoin, the system is designed to be non-inflationary on the long run.[15] When the last token is mined in such a system (as Bitcoin will be at twenty-one million), block production rewards will end. At that time, it is assumed that transaction fees will be the sole method of rewarding block production.[16] For other systems, transaction fees may be more or less important depending on the control of miners over the amount of block production awards.

C. Transaction Fee Design

Because they are paid by users for a specified service, mining transaction fees might be viewed as the private component of fiscal design in cryptocurrency systems. Even so, these fees have unexpected quasi-public features and impacts. A transaction fee may be comparable to a user fee since each participant wanting data recorded and validated must pay for the service.[17] But unlike a club charging entry fees or a state charging for toll roads or the like, the maximum amount of a transaction fee is not necessarily predetermined or predictable, and the impact of the fee payment is not limited to the person paying it.

---

13 See "Halving Countdown", *supra* note 10.

14 Some miners may have a more sophisticated view than others, and may accordingly game the system, especially in periods of uncertainty or transition such as during community standard-setting during a fork. For instance, exploiting inflationary gains appears to have motivated miners in the Bitcoin/Bitcoin cash fork: see e.g. Kyle Torpey, "How Bitcoin Cash's Higher Inflation Rate Harmed Bitcoin", *Forbes* (13 November 2017), online: <www.forbes.com> [perma.cc/P232-TKA3].

15 See Young, *supra* note 10.

16 See Nakamoto, *supra* note 1 ("[o]nce a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free" at 4).

17 See e.g. Joseph J Bambara & Paul R Allen, *Blockchain: A Practical Guide to Developing Business, Law, and Technology Solutions* (New York: McGraw-Hill Education, 2018) (explaining the concept and function of gas in the context of Ethereum, and noting that "[e]ther is needed to pay the execution cost for the Ethereum client that performs the transaction work on behalf of the sender, committing the result to the Ethereum blockchain" at 111).

In the Bitcoin model for example, the software sets minimum fees and participants may choose to pay miners more than the minimum required amount. These decisions are made individually, by reference to what the participant expects miners to be willing to accept in filling their next block with data, but a minimum amount may be designated by the miners.[18] A lower amount will almost certainly result in a delay in processing, perhaps for months. A higher amount will ensure miners' attention and be included in multiple block production such that transactions will be more likely to be verified as the blockchain lengthens.

Given the additive nature of block production, transaction fees are distinguishable from standard user fees because they have systemwide impact. That is, even though transaction fees are typically paid only to successful miners and therefore validate only those transactions associated with the fee-payors, the overall cost of processing transactions ultimately spreads throughout the cryptocurrency network as all validators incorporate the information and subsequent blocks carry validated transactions forward in time.[19]

D. System Sustainability

Together, the fee and reward system constitute a fiscal structure that is essential to the development of a successful cryptocurrency. In particular, mining must be profitable in fiat currency terms because mining requires investing in goods that can typically only be paid for in fiat currency—namely computers, the energy to run them, and the facilities to house them.[20] The profitability of mining depends on whether the tokens re-

---

18 See Josh Olszewicz, "Ethereum Price Analysis - Fees Rise with Clogged Network, Miners Respond by Raising Gas Limit" (27 September 2019), online: *Brave New Coin* <bravenewcoin.com> [perma.cc/446N-SHXD].

19 Bambara & Allen, *supra* note 17 ("transaction processing on a blockchain is not a true market because ... every transaction that the miner includes in a validated and committed block needs to be processed by every node in the blockchain network" at 109).

20 Karl J O'Dwyer & David Malone, "Bitcoin Mining and its Energy Footprint" (Paper Delivered at 25th IET Irish Signals & Systems Conference and China-Ireland International Conference on Information and Communications Technologies, 26–27 June 2014), online: *IET Digital Library* <digital-library.theiet.org/content/conferences/10.1049/cp.2014.0699> (demonstrating that profitable Bitcoin mining generally requires expensive specialized equipment and vast energy supplies). The cost to mine depends largely on the cost of electricity, which ranges widely across countries. By one estimate, the current electricity cost to mine one Bitcoin, valued at the time of this writing at US$6,400, is approximately US$3,965 in Ontario, Canada, US$4,746 in Iceland, and US$4,758 in the United States. See Jeff, "Bitcoin Mining Costs Throughout the World" (26 February 2018), online (blog): *Elite Fixtures* <elitefixtures.com> [perma.cc/L25T-HVQR]. Factoring in the cost of equipment and facilities, the profit margin on mining thus depends heavily on the current market

ceived as rewards and fees are either freely transferrable into sufficient amounts of fiat currency to cover costs and generate a profit, or directly accepted by energy companies as payment, while leaving sufficient residual to compensate the miner.

Accordingly, the viability of a blockchain-based currency system depends upon (1) the founders generating sufficient interest in the currency such that the market price exceeds the maintenance or continuation cost[21] and (2) the cryptocurrency being freely tradeable into fiat currency, at least until vendors of computers, electricity, and facilities, as well as taxing and other fee-imposing authorities accept cryptocurrency instead of fiat currency in exchange.[22] So long as these conditions are fulfilled, miners will continuously invest fiat money to mine blocks in exchange for cryptocurrency rewards.

Since block producers must receive rewards and fees in order to maintain the value of the overall network, every cryptocurrency system must necessarily introduce a system of wealth transfer to meet their expecta-

---

price of the mined cryptocurrency: see e.g. Organofcorti, "November 6th 2016 Bitcoin Network Statistics " (7 November 2016), online (blog): *Neighborhood Pool Watch: Bitcoin Mining Pool, Network, and Exchange Analysis* <organofcorti.blogspot.com> [perma.cc/KP94-ZRUW].

21 The question that the natural resources necessary to mine will continue to be accessible to miners. This is not guaranteed, since the electricity needs of miners are expansive and have overwhelmed capacity in many locations. Moreover, cryptocurrency mining is widely considered to be environmentally unsustainable, which may ultimately induce legislators to enact usage restrictions in the form of outright bans or fees that would preclude profitability. See O'Dwyer & Malone, *supra* note 20 (that the energy used for Bitcoin mining is equivalent to the annual energy consumption of the population of Ireland); CRS Report, *supra* note 1 ("[i]n addition to raising questions about whether cryptocurrencies ultimately will be more efficient than existing payment systems, such high-energy consumption could result in high *negative externalities*—wherein the price of a market transaction, such as purchasing electricity, may not fully reflect all societal costs, such as pollution from electricity production" at 14).

22 Some governments have indicated a willingness to accept tax payments in Bitcoin: see e.g. David Z Morris, "Arizona Senate Votes to Accept Tax Payments in Bitcoin", *Fortune* (10 February 2018), online: <fortune.com> [perma.cc/J8RV-Q6CC]; Becky Peterson, "A Controversial Florida Politician Just Made His County the First in the US to Let Residents Pay Taxes with Bitcoin" *Business Insider* (14 May 2018), online: <businessinsider.com> [perma.cc/E2TD-USWU]. Others have rejected legislation to do so: see e.g. Kelly Phillips Erb, "Ask the Taxgirl: Paying Your Taxes With Bitcoin", *Forbes* (16 January 2018), online: <www.forbes.com > [perma.cc/U6DN-W9SW]. Currently, digital cash (such as Bitcoin) is the only commercially successful application of blockchain technology. See e.g. Saifedean Ammous, "Blockchain Technology: What is it good for?" (2016) at 4–6, online: *SSRN* <ssrn.com/abstract=2832751> (comparing blockchain to current technologies in the financial industry and revealing barriers to the successful commercial implementation of blockchain, including costly redundancies and irreversibility, serious scaling problems, and non-compliance with state regulatory systems).

tions. The fiscal choices made to effectuate such transfers is, in effect, the internal tax system of blockchain—that is, its tax *cryptographia*.

Like the larger *lex cryptographia* of which it constitutes an essential element, tax *cryptographia* is built in to a particular cryptocurrency system via coding and protocol updates but it is subject to perpetual renegotiation by the participants.[23] The same definition could be applied to taxation by the state: written into codes, taxation rules are so important to the economic and social functioning of societies, and so impactful on the lives of individuals subjected to them, they become permanent features of the political landscape everywhere they are imposed.[24] Accordingly, the next section undertakes an explicit comparison of tax *cryptographia* to state-based taxation.

II. Blockchain's Fiscal Logic: Is It Taxation?

This Part examines why the fiscal structure of cryptocurrencies might be analyzed as a form of taxation. This characterization is significant in governance terms precisely because cryptocurrencies are so often promoted as permitting their participants to break free from the coercive power of the state. If cryptocurrency developers effectively recreate state-like conditions for their participants by redistributing participants' wealth to fund goods of value to all, then the same political struggles that attend to state governance efforts, especially taxation, arise in the context of cryptocurrencies.[25] Because miner compensation is an essential element of every cryptocurrency, and because the act of mining produces what amounts to a quasi-public good internal to the particular cryptocurrency, this Part concludes that cryptocurrency founders are inescapably in the business of recreating what amounts to taxation systems, with attendant policy ramifications.

---

[23] See Wright & De Filippi, *supra* note 6; see also Olszewicz, *supra* note 18 (explaining continuous protocol updating with respect to Ethereum).

[24] The literature on the political nature of taxation by the state is vast. For a broad overview, see generally B Guy Peters, *The Politics of Taxation: A Comparative Perspective* (Cambridge, MA: Basil Blackwell, 1991). For a look at how taxation policy develops through recursive iterations of regulatory, interpretive, and judicial interactions, see generally Allison Christians, "Historic, Comparative and Evolutionary Analysis of Tax Systems" in Misabel Abreu Machado Derzi, ed, *Separação de Poderes e Efetividade do Sistema Tributário* (Belo Horizonte: Del Ray Press, 2010) 287.

[25] For an account of the comparison of non-state communitarian efforts to the actions and motivations of states, see e.g. Michael Walzer, *Spheres of Justice: A Defense of Pluralism and Equality* (New York: Basic Books, 1983) at ch 2. For an explanation of the economics of club goods, see Todd Sandler, "Buchanan Clubs" (2013) 24:4 Constitutional Political Economy 265 at 267–68 (examining the distinction between club goods and public goods).

A. Mining is Obligatory

As outlined above, in designing a cryptocurrency, incentivizing block production is a threshold consideration because if mining is not profitable, transactions in the currency will not be recorded, trading will stop, the value of the currency will plummet, and the cryptocurrency system as a whole will fail.[26] May transaction fees and block production rewards thus be seen to take on tax-like functions in the blockchain space? The voluntary nature of participation in a given cryptocurrency might suggest not, since taxation is typically defined as the compulsory transfer of resources among members of society.[27] Yet cryptocurrency founders must violate the economic freedom of participants to some extent to ensure miners will be amply rewarded for their infrastructural contributions. Like conventional legal orders, cryptocurrency systems inevitably appropriate to common purposes specified property that would otherwise accrue to private ownership. Conventional taxation does so through constitutions and laws, whereas cryptocurrency taxation does so with computer code.

Clearly the coercive power of the state to control human movement in and out of the system it creates is relevant and makes cryptocurrency fiscal design a fundamentally different project than state-level governance. It is relatively easy to buy into and out of one cryptocurrency or another, while physical borders backed by police and military powers more forcibly restrict a person from moving between autonomous sovereign territories. Still, there are important parallels. The extraction of resources from some to pay others is not voluntary within a cryptocurrency system in the same way that it might be in another market exchange environment. This is because the costs to users are not borne as service fees to a specific entity such as a business but as part of the total environment. Further, the benefits of transaction validation are not confined to those engaging in specified transactions but are system-wide.

As such, there are some strong similarities between what cryptocurrency founders are doing in incentivizing block production, and what states do when they are organizing themselves.[28] States typically have to

---

[26] See Tang & Chow *supra* note 9 (explaining that "in most cryptocurrency projects, the total amount of coins (including coins to be minted) is predetermined. A certain fraction of coins is initially offered to the team of the project, as well as early investors when the system is started. Afterward, another fraction of coins is offered to a decentralized autonomous organization (DAO). Finally, remaining coins are reserved for miners to motivate them for generating a new block. These coins will eventually be all minted" at 62).

[27] See Christians, "Drawing the Boundaries", *supra* note 5.

[28] The metaphysical nature of taxation continues to intrigue scholars, policymakers and practitioners alike, as evidenced by the inclusion of the topic in influential internation-

find a means to establish control over a physical territory and a people.[29] They use taxes (although not necessarily exclusively) to pay individuals to govern as legislators, judges, and law enforcers, to build government buildings and related infrastructure, and to wage war against other societies, whether in aggression (to gain territory or resources) or to defend against aggression from other societies.[30]

Similarly, although cryptocurrency founders need not defend a physical territory, they clearly must establish a digital territory and then defend it against attacks. When they fail to do so in the eyes of enough of their participants, they will face social fracture, such as Ethereum did in a highly publicised event in 2016.[31] It is therefore probably uncontroversial to conclude that cryptocurrency founders, before doing anything else, must find a way to incentivize mining of their token. It might be more controversial to suggest that this activity amounts to anything more than a set of private market transactions, but there are reasons to conclude that, in fact, mining effectively produces something like public goods within the system it helps to build.

---

al conferences such as that hosted annually by the International Fiscal Association: see Marjaana Helminen, "General Report" in International Fiscal Association, *The Notion of Tax and the Elimination of International Double Taxation or Double Non-taxation* (Paper delivered at the Congress of the International Fiscal Association, Madrid, 25-30 September 2016) (The Hague: Sdu Uitgevers, 2016) 17 (examining historical and ongoing lack of consensus on what constitutes taxation and stating that "The following four elements of tax seem to be recognized in most states in one form or in another. A tax is a (a) compulsory levy, which (b) is imposed by an organ of government (c) for public purposes (d) without regard to the particular benefits received by the taxpayer (unrequited payment)" at 22 (citations omitted)). See also Nigel Dodd, *The Social Life of Money* (Princeton, New Jersey: Princeton University Press, 2014) at 4, 24 (making the case for an inseverable connection between the state's control of monetary policy and its power to tax by explaining that "[t]he right to create money raises profound questions about power, freedom, justice, and law" and noting that "monetary theorists who claim that money's origins are political and religious, not commercial. *Geld* derives from *gild*, meaning tax, and both words resonate with the old Icelandic *gjald* (recompense, punishment, payment) and the old English *gield* (substitute, indemnity, sacrifice). The etymology supports those who argue that money's roots lie not just in debt but in a particular *kind* of debt. This debt is payment to an authority...").

29 For a classic explanation, see Adam Smith, *An Inquiry into the Nature and Causes of the Wealth of Nations*, vol 3 (London: Printed for William Allason, J Maynard & W Blair, 1819) ("[t]he first duty of the sovereign, that of protecting the society from the violence and invasion of other independent societies, can be performed only by means of a military force" book 5 at 69).

30 See generally Christians, "Drawing the Boundaries", *supra* note 5.

31 Discussed *below* at note 34.

B. Mining Produces a Quasi-Public Good

Cryptocurrency mining is clearly undertaken for private gain, but there is an altruistic outcome to the collective effort of miners, namely, the maintenance and value enhancement of the blockchain as a whole. This makes mining comparable to the government function of providing public goods, such as physical infrastructure and defence.[32] The question is whether the comparison is apt and if so, what the standard cryptocurrency mining compensation structure might tell us about its governance design.

Mining creates value by creating a virtuous cycle between transacting in the mined currency and generating new blocks. As currency holders exchange with others (whether for other cryptocurrencies or fiat currencies), they create information that has no value unless it is mined into successive blocks. By mining, miners enable currency transferability and therefore contribute to the value of the currency for everyone.[33] But mining creates value in a more essential way, that is, by implementing blockchain governance decisions in the form of software updates. Individual members might not be aware of or interested in these governance decisions, but the distribution of software updates is key to the proliferation of the blockchain.[34]

In brief terms, economists distinguish public goods from private goods based on excludability and use. For example, a classic textbook definition explains that public goods exist because "[i]t is generally considered impossible to exclude those who refuse to pay voluntarily for public services, such as defense or police protection, from consuming these services."[35]

---

[32] There is also a lot of waste generated in mining, in the form of fiat money spent on the electricity used to mine unsuccessful blocks. It is worth considering how this wasteful spending by private procurers should be counted, especially given the environmental externalities.

[33] Whether the act of mining is in fact value-creating is debatable in contemporary terms. The sole commercial success of blockchain technology to date is the production of digital cash and facilitation of transfers thereof. No blockchain application without currency has yet to move from the prototype stage to commercial implementation.

[34] A relatively well-known example is in the act of "forking" a blockchain when participants disagree on basic governance decisions, as occurred in the distributed autonomous organization DAO, a public investment fund hosted on the Ethereum blockchain. See Morgan E Peck, "DAO May Be Dead After $60 Million Theft" (17 June 2016), online: *IEEE Spectrum* <spectrum.ieee.org> [perma.cc/8Y3L-4YKP]; Morgen E Peck, ""Hard Fork" Coming to Restore Ethereum Funds to Investors of Hacked DAO" (19 July 2016), online: *IEEE Spectrum* <spectrum.ieee.org> [perma.cc/FS9V-6HV7].

[35] Walter Hettich & Stanley L Winer, "Rules, Politics, and the Normative Analysis of Taxation" in Jürgen G Backhaus & Richard E Wagner, eds, *Handbook of Public Finance* (Boston: Kluwer Academic, 2004) 109 at 111.

Thus in general, "non-rivalrous" goods or services are those that are not depleted by use, while "non-excludable" goods or services are those that cannot be furnished to some, without being furnished to all.[36]

A quintessential example of a non-rivalrous and non-excludable service is a state's use of military force to protect against would-be foreign invaders. It would be virtually impossible for such national security efforts to protect only some members of the state, while leaving others vulnerable to attack. Provided for one against an outside threat, military defense protects all.[37] This is the essential nature of cryptographic mining: provided for one transaction or a set of transactions, successful mining creates the means for additional trustless transactions, protecting all participants against fraud.

Moreover, blockchain protection of all the participants comes at no cost. As opposed to conventional state protection in a physical world, where the cost of protection is quite high, in the digital realm, the cost of protection has zero marginal cost.[38] Software code is easily copied, modified, and spread at high speed to every computer of the network, ensuring that every participant follows the longest and strongest chain. The digital

---

[36] See generally Paul A Samuelson, "The Pure Theory of Public Expenditure" (1954) 36:4 The Review of Economics and Statistics 387.

[37] When goods or services are both non-rivalrous and non-excludable, economists worry about free-riding, or the likelihood that people will benefit from services for which they do not pay, which usually means they impose a cost on someone else. In contrast, some rivalrous and excludable goods and services include police protection, firefighting, clean water, parks, roads, and so on. In this regard, we may turn to examples from US jurisdictions where fire-fighting services are based on an annual fee. When a fire occurs at a residence where the fee is not paid, protection will be afforded to the surrounding houses for which fees were paid, but the fire service will not put out the blaze at non-payor's house, allowing it to burn to the ground: see e.g. "Firefighters Let Home Burn Over $75 Fee -- Again" (7 December 2011), online: *NBC News* <usnews.nbcnews.com> [perma.cc/A98V-R2ZF] ("[f]irefighters stood by and watched a Tennessee house burn to the ground earlier this week because the homeowners didn't pay the annual subscription fee for fire service. ... The city makes no exceptions. 'There's no way to go to every fire and be able to keep up the manpower, the equipment, and just the funding for the fire department,' said South Fulton Mayor David Crocker"). This outcome generates public consternation and even outrage on occasion, but the rationale is that if persons could receive fire protection without paying their dues, or if they were allowed to pay their dues upon the occasion of a fire occurring at their residence, no one would pay the annual fee and the service would cease to exist. Economists describe this as a situation involving "moral hazard". See e.g. Paul Krugman, The Return of Depression Economics and the Crisis of 2008 (New York: W.W. Norton & Company, 2009) (describing moral hazard as "any situation in which one person makes the decision about how much risk to take, while someone else bears the cost if things go badly" at 63).

[38] See generally Jeremy Rifkin, *The Zero Marginal Cost Society: The Internet of Things, the Collaborative Commons, and the Eclipse of Capitalism* (New York: Palgrave Macmillan, 2014).

nature of blockchain protection offers a higher degree of adaptability and malleability in case of an attack.

C. Tax Cryptographia Emerges

Because they use voluntarily established fees and variable rewards to maintain their systems, some might reject what cryptocurrency founders do as taxation. But not everything a state does to fund a government is immediately recognizable as taxation either. For example, many states raise funds by licensing or selling state-controlled resources,[39] by directly owning the means of production,[40] by interjecting themselves as a sole buyer of domestic goods or services,[41] by printing money, and by borrowing funds.[42]

Even though these policy choices may not be classically viewed as "taxation" in the formal sense, each of these activities has the same effect as taxation in the sense that each places resources under the direct control of those making governance choices, and beyond the reach of individuals.[43] Each might be characterized as economic equivalents to taxation,

---

39 For example, licensing mining or logging rights, or selling land outright.

40 This can be accomplished either by directly owning and operating businesses (via state-owned enterprises) or by owning a stake in private businesses (such as through a sovereign wealth fund).

41 Such as in a monopsony (a market with many sellers but only one buyer). Many states use or have used law to create a monopsony in order to control agricultural and natural resource sales, whether to extract a tax, control exports, or both. The Canadian Wheat Board, established in 1935, had a monopsony as the sole legal buyer of wheat and barley produced in Canada, until the law was changed in 2012. See *Marketing Freedom for Grain Farmers Act*, SC 2011, c 25.

42 Borrowing is not itself a tax in the sense that it is not compulsorily imposed, and its economic impact on current and future generations is debated. However, borrowing generally requires paying interest and principal, which requires taxation in some form (barring the possibility of perpetually borrowing in order to pay off prior borrowing).

43 See Helminen *supra* note 28 at 22–23 (noting that "[t]he notion of tax is not easy to define exhaustively," that "most states' statutes do not include an express definition," and that there is no international consensus on the term); Henk Vording, "The Normative Background for a Broad Concept of Tax", in Bruno Peeters et al, eds, *The Concept of Tax* (Amsterdam: EATLP, 2005) 30 at 46–47 (discussing the complex borderline between taxes and other fees, especially in the context of compulsory national social insurance schemes); Mark Bowler Smith & Huigenia Ostik, "Towards a Classification of the Central London Congestion Charge as a Tax" (2011) 4 Brit Tax Rev 487 at 487, 489 (outlining the "difficulty in determining whether a given payment is classifiable as a tax or a user charge in anything but the most clear-cut cases," noting that "[i]n the literature, 'charge levied for specific services rendered', 'user charge', 'user fee', 'payment for government service' and 'sale of a service' are defined by similar, and sometimes identical, classification criteria and are often used interchangeably", and stating that "voluntariness, regulatory purpose and hypothecation are less helpful as classification

indirect forms of taxation, or taxation by another name. Many of these activities describe what founders effectively do when they design incentives to ensure block production and investment in their cryptocurrencies.[44]

Despite the libertarian leanings that have driven enthusiasm for cryptocurrency to date, it should not be surprising that the development of quasi-public goods and the means to pay for them through required contributions are two fundamental aspects of cryptocurrency systems. Tax *cryptographia* emerging from these design decisions provides some affirmation of the notion that fiscal policy is key to building virtually any complex form of society, even when the designers expressly sought an alternative to the coercive power of the state.[45]

III. A Policy Assessment of Tax Cryptographia

If the foregoing characterizations of cryptocurrency fiscal policy choices are apt, then tax *cryptographia*'s essential nature appears to be inflationary in some cases while being regressive in virtually all cases. In state-based tax systems, these two features would likely produce strong public opposition, leading to political turnover. But in cryptocurrency systems, strong opposition leads to dissent, fracture, and on occasion total systemic failure.[46] Whether cryptocurrency founders are learning or will

---

criteria of a user charge than the need to establish the existence of an identifiable service and proportionality between the service and the payment" (citations omitted)).

44 In particular, releasing block rewards is most similar to the exercise of printing money, which can act as a form of taxation by creating inflation. For a discussion on inflation as a form of taxation, see generally Andrés Erosa & Gustavo Ventura, "On Inflation as a Regressive Consumption Tax" (2002) 49:4 J Monetary Economics 761.

45 The enthusiasm of blockchain proponents to avoid replicating the state is merely the latest in a long line of pseudo-libertarian projects that promised similar utopian outcomes only to either entrap prospective members in an equally regulated but less democratic social order or to subject them to various kinds of fraud, or both. Examples of such projects include the failed "Galt's Gulch" project in Chile, which promised investors an anarcho-libertarian life free of state regulation but delivered a dubious real estate scheme that violated local zoning laws and ended in protracted litigation among the founders and investors in state courts: see Brian Hutchinson, "'Freedom and Liberty' not Enough to Save Galt's Gulch Chile Libertarian Community from Bureaucracy and Internal Dissent", *National Post* (26 September 2014), online: <nationalpost.com> [perma.cc/2D6Y-A6S3]; Harry Cheadle, "Atlas Mugged: How a Libertarian Paradise in Chile Fell Apart", *Vice* (22 September 2014), online: <www.vice.com> [perma.cc/FT7W-L5B5] (after offering "respite from the Western world of oppressive governments to freedom-minded people in which they can build a new, more prosperous community," the founders of Galt's Gulch Chile became mired in conflict and accusations of fraud).

46 Even absent failure, de facto centralization can occur without any governance mechanisms to prevent misuse of power. For example, the increasing cost of mining Bitcoin favors large mining operations and crowds out smaller players, thus increasing the risk that a core group of miners might gain sufficient power to control the system. See

learn from the vast experience of taxation within political organizations remains to be seen.

A. Often Inflationary, Inherently Regressive

Tax *cryptographia* is often inflationary in the sense that when undertaken by a state, printing money to pay for public goods is understood to extract value from the members of society by devaluing their currency and therefore making it more expensive to exchange the currency for other goods. Producing inflation can have distributional effects similar to taxation in that it can move economic value from some community members to others in order to create a good to be shared by all. In the case of cryptocurrency, the block reward allowance to miners is equivalent to printing money, and the quasi-public good is the continuation of the blockchain that makes the currency tradeable for everyone.[47] In a conventional society, inflationary policy will presumably be accepted so long as existing holders will accept the periodic dilution of their currency because they believe that the policy will increase the value to all holders in the long run; presumably the same logic extends to cryptocurrency systems.[48]

It is worthwhile examining the temporal nature of blockchain production rewards where the founders have set a finite number of tokens to be produced, thus setting a limit on the built-in capacity for inflation. This is the case for Bitcoin, which has been designed to reach an upper limit of twenty-one million. The enforced cap is seen as infrastructural protection against inflation. Yet given the high cost of Bitcoin block production, without an alternative plan in place, the end of rewards will result in an escalation of transaction fees.

O'Dwyer and Malone, *supra* note 20; Arthur Gervais et al, "Is Bitcoin a Decentralized Currency?" (2014) 12:3 *IEEE Security & Privacy* 54 (outlining a lack of transparency in decision making and arguing that the privileged position of code developers and miners makes Bitcoin an effectively centralized system). See also Urs Gasser, Ryan Budish & Sarah Myers West, "Multistakeholder as Governance Groups: Observations from Case Studies" (2015), Berkman Center Research Publication No 2015-1; Nicolas Courtois, "On the Longest Chain Rule and Programmed Self-Destruction of Crypto Currencies" (2014), online (pdf): *ResearchGate* <researchgate.net> [perma.cc/9BL9-G7NB].

47 The inflationary nature of providing cryptocurrency rewards in exchange for mining is explored in Tang & Chow, *supra* note 9 ("[a]n increase in the number of existing coins can lead to a decrease in value per coin, i.e., inflation, and motivate transactions ... To our knowledge, almost all cryptocurrency systems up-to-date incur an increase in the total number of coins for block generation. The rate of inflation for all blockchain-based cryptocurrency systems is predetermined when the system is designed" at 61).

48 Valuation is a sensitive subject in cryptocurrency analysis, with volatility and speculation the dominant characteristics.

The transaction fee structure makes tax *cryptographia* appear inherently regressive, perhaps especially in the absence of inflation as an alternative payment system. The cost of transaction validation is typically imposed as a flat fee, such that those with fewer assets must pay the same to have their transactions recorded as those with much more. This is regressive in the economic sense that it defies the impact of the declining marginal utility of money, that is, the utilitarian theory that the value per unit of money declines, the more one has of it.[49] Thus in common terms, a single dollar means a great deal to a person who has very little, but it means much less to a very wealthy individual.

The possibility of paying a higher fee to accelerate the validation of certain transactions makes tax *cryptographia* additionally regressive, while also negating the egalitarian attraction of blockchain in more general terms. Those capable of paying higher fees accelerate or privilege their transactions over others, creating a de facto hierarchy within the decentralized network. Because of their authority in maintaining the ongoing viability of the blockchain, miners can use the versatile fee structure to assert their authority and preferences without warning, review, or redress.[50]

In the near term, the impact of the inflationary and regressive nature of tax *cryptographia* is unclear and may be negligible. To date the value of existing cryptocurrency tokens appears largely independent of inflationary policy.[51] Speculation and herding behaviours by investors, imperfect public perceptions, market competition and the cost of block production appear to be key price determinants.[52] Even so, researchers find that the

---

49 For the origins of marginal utility theory, see generally Jeremy Bentham, *Introduction to the Principles of Morals and Legislation*, revised ed (Kitchener: Batoche Books, 2000); Hermann Heinrich Gossen, *The Laws of Human Relations and the Rules of Human Action Derived Therefrom*, translated by Rudolph C Blitz (Cambridge, Mass: MIT Press, 1983).

50 See generally Francesca Musiani, "Governance by Algorithms" (2013) 2:3 Internet Policy Review 1; Torpey, *supra* note 14.

51 For example, as Alan Greenspan quipped, "[y]ou have to really stretch your imagination to infer what the intrinsic value of Bitcoin is. I haven't been able to do it. Maybe somebody else can." See Jeff Kearns, "Greenspan Says Bitcoin a Bubble Without Intrinsic Currency Value" (4 December 2013), online: *Bloomberg* <bloomberg.com> [perma.cc/GWS5-YDY7].

52 See Halvor Aarhus Aalborg, Peter Molnár & Jon Erik de Vries, "What can Explain the Price, Volatility and Trading Volume of Bitcoin?" (2019) 29 Finance Research Letters 255 (finding that Bitcoin pricing depends on a combination of factors, none of which can predict its returns, including "traded volume at Bitcoin exchanges, transaction volume in Bitcoin network [and] the number of unique Bitcoin addresses and Google searches for the term 'Bitcoin'" at 256); Adam S Hayes, "Cryptocurrency Value Formation: An Empirical Study Leading to a Cost of Production Model for Valuing Bitcoin" (2017) 34:7

major cryptocurrencies, especially Bitcoin, continue to be perceived as viable investments, including in terms of balancing a diversified portfolio and hedging risk.[53] Moreover, cryptographic technology is an innovative development that continues to attract attention and investment, and is likely to evolve rather than disappear.[54] If so, the fiscal policy of cryptocurrency will likely evolve as well.

B. Tax Cryptographia is Inevitable

The likely future development of cryptocurrency technology implies that some form of redistribution is inevitable, whether or not characterized as taxation. This is consistent with the idea that taxation is more or less inevitable to build virtually any functioning cooperative enterprise, whether within the concept of a nation-state or otherwise. For example, Robert Nozick demonstrated that all builders of complex polities will cooperate to fund a basic set of public goods in order to make it possible for

---

Telematics and Informatics 1308 (proposing a regression model to estimate the value of Bitcoin by reference to the level of competition in the producer network, the rate of unit production, and the difficulty of algorithm used to mine for the cryptocurrency); Minul Wimalagunaratne & Guhanathan Poravi, "A Predictive Model for the Global Cryptocurrency Market: A Holistic Approach to Predicting Cryptocurrency Prices" (Paper delivered at the 8th International Conference on Intelligent Systems, Modelling and Simulation, Malaysia, 8-10 May 2018) 78 (stating that "the cryptocurrency market is highly unstable and experiences periods of extreme volatility which often makes it difficult to predict behavioral patterns" (at 78) and examining the connection between cryptocurrency prices and public perception gleaned through online and social media); Nidhaleddine Ben Cheikh, Younes Ben Zaied & Julien Chevallier, "Asymmetric Volatility in Cryptocurrency Markets: New Evidence from Smooth Transition GARCH Models" (2019) Finance Research Letters 1 (describing volatility in cryptocurrency pricing and noting that "Bitcoin, as the most popular and traded cryptocurrency, has experienced extreme fluctuation since its introduction in 2009," experiencing "[l]arge occasional price swings, such as the market crash of December 2013 and the unprecedented price levels in late 2017" at 1); Nils Bundi & Marc Wildi, "Bitcoin and Market-(in)efficiency: a Systematic Time Series Approach" (2019) 1:4 Digital Finance 47 at 48 (noting extreme price volatility due to information asymmetry and other market distortions and concluding that cryptocurrency markets are not in fact becoming more efficient over time).

53 See David Lee Kuo Chuen, Li Guo & Yu Wang, "Cryptocurrency: A new investment opportunity?" (2018) 20:3 Journal of Alternative Investments 16; Anne Haubo Dyhrberg, "Bitcoin, Gold and the Dollar – A GARCH Volatility Analysis" (2016) 16 Finance Research Letters 85.

54 See e.g. Sarah Hansen, "New Report: 70% Of Finance Execs Believe Cryptocurrency Is Here To Stay", *Forbes* (12 September 2018), online: <www.forbes.com> [perma.cc/FZS5-46KQ] (discussing an industry report that consulted 141 institutional investment executives and found that over 70% of such executives believe "that a regulatory framework will develop around cryptocurrencies, leading to growth and innovation").

them to function as a society.[55] He referred to the society that agrees to a minimal set of basic public goods—the minimal or "night-watchman" state—as essentially redistributive because the necessary commitment involved assigning a monopoly over violence to a collectively approved government, thus pooling resources to pay for security.[56]

The baseline of Nozick's framework for cooperation in a night-watchman state is a pre-existing physical world. In physical terms, resources exist, and people are capable of manipulating, managing, recreating, and adding value to them. But to do so effectively and continuously requires removing violence from the market as much as possible, to ensure that exchanges can take place without distortions caused by compulsion. Thus, Nozick posits that anyone seeking to create a free market must replace a state of nature featuring survival of the fittest with a negotiated society that creates and protects the means for trade by removing the threat of physical violence.[57]

In a cryptocurrency system, it might seem that there is no need for night watchmen because decentralization has eliminated the need for trust as a matter of governance. However, as shown above, it is vitally necessary to produce the means for undertaking value-creating activity by producing software updates which are disseminated and effectuated (such as through mining). Even when characterized as general-purpose in

---

55 See generally Robert Nozick, *Anarchy, State and Utopia* (Oxford: Blackwell, 1974). This intuition is supported by political theorists who conclude that but for taxation, there can be no market for free exchange, such that taxation should not be considered an extraction of resources but rather a necessary precondition, albeit one we usually associate with the state. This is the basic message of, for example, Liam Murphy & Thomas Nagel, *The Myth of Ownership: Taxes and Justice* (Oxford: Oxford University Press, 2002) (making the case that the state facilitates the market and the means for private income-earning transactions to take place, so the imposition of taxes should not be viewed as an interference with private property rights).

56 Nozick, *supra* note 55 (stating that "[t]he night-watchman state of classical liberal theory, limited to the functions of protecting all its citizens against violence, theft, and fraud, and to the enforcement of contracts, and so on, appears to be redistributive" at 26).

57 See *ibid* ("[t]o get to something recognizable as a state we must show (1) how an ultraminimal state arises out of the system of private protective associations; and (2) how the ultraminimal state is transformed into the minimal state, how it gives rise to that 'redistribution' for the general provision of protective services that constitutes it as the minimal state. To show that the minimal state is morally legitimate, to show it is not immoral itself, we must show also that these transitions in (1) and (2) *each* are morally legitimate. ... We argue that the first transition, from a system of private protective agencies to an ultraminimal state, will occur by an invisible-hand process in a morally permissible way that violates no one's rights. Secondly, we argue that the transition from an ultraminimal state to a minimal state morally must occur. It would be morally impermissible for persons to maintain the monopoly in the ultraminimal state without providing protective services for all, even if this requires specific 'redistribution'" at 52).

nature, the design of these updates will ultimately dictate the behaviour of the users. In every update, political choices are embedded into the code, whether intentionally or not.[58] Different codes have distinct consequences on the network as a whole, supporting certain code structures or facilitating certain actions over others.[59]

Accordingly, there is a strong case to be made that cryptographic mining is akin to a public good in terms of its construction of the basic means necessary to maintain the cryptocurrency and potentially to increase its value over time. If so, then the system of rewards and fees for miners can be compared to a tax system which distributes costs and benefits to the participants within the system. The choices made by cryptocurrency founders to date are often inflationary and typically regressive. They also seem unsustainable, as fees and rewards may be eclipsed by the cost of mining in the face of speculation-induced price volatility.[60] It remains to be seen whether these fiscal choices will be acceptable in the long run, and if not, whether cryptocurrency founders, miners, and investors will be capable of designing alternative fiscal systems that will be agreeable as well as sustainable.

Conclusion

Technological change has always offered both challenge and opportunity for achieving social goals through regulation. The emergence and

---

58 See Primavera De Filippi & Benjamin Loveluck, "The Invisible Politics of Bitcoin: Governance Crisis of a Decentralized Infrastructure" (2016) 5:3 Internet Policy Review 1 ("Bitcoin embodies in its very protocols a profoundly market-driven approach to social coordination, premised on strong assumptions of rational choice and game- theoretical principles of non-cooperation" at 5).

59 See Primavera De Filippi & Samer Hassan, "Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code" (2016) 21:12 First Monday. De Filippi and Hassan describe blockchain governance design as akin to urban planning, observing that many cities organize their roads in such way as to conceal the view of slums from the city center or preclude people from sleeping on public benches (*ibid*). These choices reflect the preferences of the wealthy and ignore the needs of those with less power to control their environment, thus entrenching unequal social order. See also Neil Smith, *The New Urban Frontier: Gentrification and the Revanchist City* (London: Routledge, 1996) at 5. This is also the basic lesson of Lawrence Lessig's claim that "code is law" (*Code*, 2nd ed (New York: Basic Books, 2006) at 1–8).

60 See Atulya Sarin, "Opinion: Bitcoin is Close to Becoming Worthless", *MarketWatch* (4 December 2018), online: <www.marketwatch.com> [perma.cc/XMZ8-DTFQ]:

> [O]nce Bitcoin's price falls below its cost of mining, the incentive to mine will deteriorate, thrusting bitcoin into a death spiral. That is, without the mining activities supporting the ledger that maintains the records of who owns what—bitcoin is, after all, a set of encrypted numbers that cannot establish the ownership of anything—bitcoin will become worthless.

widespread adoption of innovations like cryptocurrency raise traditional regulatory concerns, such as how to effectively regulate public risk through securities law and social contribution through tax law. But because of their unique nature, cryptocurrencies also raise particularly interesting internal governance questions for innovators and consumers, including how decisions about costs and benefits are made within new platforms and modes of commercial and investment activity.

From the conceptualization of cryptocurrencies in the late 2000s through the initial coin offering frenzy of 2017, followed by a sobering revelation of the difficulties involved in practical application for everyday uses beyond the production and marketing of heavily speculative cryptographic assets, most of the legal questions being asked by and about cryptocurrency have been practical ones.[61] They focus on how this technology challenges and is challenged by existing regulatory frameworks and how innovators, investors, and consumers manage regulatory risk. Broader questions about how cryptocurrency developers establish internal governance structures have only recently begun to emerge in scholarship.

Studying the internal governance decisions of cryptocurrency founders and designers helps explain the motivations of the parties in a cryptocurrency system and potentially tells us something about how we understand traditional rule of law processes (and how common perceptions may be changing regarding the rationale of the rule of law). Further, the centuries of study that have shaped the development of modern democratic societies inform (or should inform) cryptocurrency innovators about likely pressures on their decision making. Age-old struggles over tax law ought to be relevant to developers because these experiences have taught societies over and over again that the manner in which funds are pooled and spent on common projects is key to their viability.

Taxation is particularly fascinating to consider in cryptocurrency systems because of the libertarian roots that helped propel widespread enthusiasm for cryptocurrencies. The U.S. Supreme Court case of *McCulloch v. Maryland* is often cited by libertarian enthusiasts for the famous observation that the power to tax is the power to destroy.[62] But in cryptocurrency systems, the inability to tax likely has a similar result. For today's cryptocurrency founders, investors and consumers, the decisions

---

61 As documented in Cheikh, Zaied & Chevallier, *supra* note 52. The general lack of attention to core governance questions is noted in Tang & Chow, *supra* note 9 ("[t]o our knowledge, the methodology of eliminating coins, or even the inflation and the deflation of cryptocurrencies, are never considered in the cryptocurrency literature" at 61).

62 17 US (4 Wheat) 316 (1819). The precise text states, "[a]n unlimited power to tax involves, necessarily, a power to destroy," thus including a parameter not typically recalled in the popular narrative (*ibid* at 327).

made about how to share the costs of basic goods among participants involves a difficult governance question that has vexed governments throughout the ages. To date, it seems that these lessons are largely being ignored. The consequences for the long term viability of applied cryptocurrency technology are yet to be seen.