Jacob Bendicksen

Joan Feigenbaum

CPSC 610

December 13, 2019

Bitcoin as Common-Pool Resource: Applying Ostrom's IAD Framework to Cryptocurrency

When one thinks of common-pool resources, things like fish stocks, forests, and grazing lands usually come to mind. This makes sense—Garrett Hardin's "Tragedy of the Commons" used grazing land as its prototypical example[1]—and most analyses of common-pool resources focus on physical resources. These analyses tend to be difficult to compare as a result of the wide variation in resources and appropriation systems, and for this reason, Elinor Ostrom developed the Institutional Analysis and Development (IAD) framework.[2] The IAD framework standardizes the analysis of common-pool resource appropriation systems, and scholars have begun to see its utility in domains beyond physical resources. Recent analyses have looked at various aspects of the internet,[3] and this paper will focus on another internet resource: Bitcoin.

Over the past several years, few ideas from the world of computer science have captivated the broader world in the way that Bitcoin has, but the currency's instability has likely prevented more widespread adoption. This volatility does not appear to have been a desirable outcome to Bitcoin's pseudonymous creator, Satoshi Nakamoto, because he designed Bitcoin as a currency,[4] rather than an investment vehicle. (No one ever talks about 'investing in the US dollar' in the same way that they might talk about 'investing in the stock market.') Volatility

---

[1] Hardin, "The Tragedy of the Commons," 1244.
[2] Polski and Ostrom, "An Institutional Framework for Policy Analysis and Design."
[3] Shackelford, "Governing the Internet of Everything"; Morell, "Governance of Online Creation Communities."
[4] Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 1.

never comes up in the original Bitcoin white paper.[5] The problem appears to be that people formerly unfamiliar with Bitcoin hear about it as a rapidly appreciating asset and buy it through payment intermediaries and online wallets, such as Coinbase,[6] then sell at the first sign of trouble. Given that these users often do not become involved in the Bitcoin community beyond buying and selling, they are not invested in the long-term health and stability of the resource in the same way that miners are. The increase in popularity has also resulted in bad outcomes for miners: given that the system holds the rate of Bitcoin production constant by adjusting the hash difficulty,[7] the growing numbers of miners results in smaller rewards per miner. Neither of these outcomes appear satisfactory for the long-term health of the system, and the rest of this paper will attempt to explain why they happen in more detail. This will begin with a description of the attributes of the system and community, then a discussion of the rules-in-use, then analyze Bitcoin's compliance with a set of design principles proposed by Ostrom.

Physical and Material Conditions

The Bitcoin system physically manifests itself in the computers that mine and sell Bitcoin, and as an internet-native system, it exists globally. As a currency, it is a private good, produced through mining and distributed over the internet. Its scope is limited to the production and distribution of Bitcoins. The necessary physical components for actors in all roles are electricity, a computer, and an internet connection, but other dependencies differ depending on role. Miners need to know how to run a node, while intermediaries need to know how to run a business, and users need to know very little. Similarly, miners need mining code and

[5] Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System."
[6] https://www.coinbase.com
[7] Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 3.

intermediaries need payments infrastructure, while users need no technologies beyond an internet-capable device. Finally, on the topic of processes, miners need the mining algorithm and the consensus protocol, intermediaries need payment protocols, and users need nothing. Storage requirements can be substantial for miners who need to hold the entire blockchain in memory,[8] but insignificant for intermediaries and users who only need to deal with their individual states. Distribution is not hard with a reasonable internet connection.[9]

Community Attributes

The Bitcoin community is diverse in location but not beliefs. There were 872,000 distinct nodes in 2014,[10] and Bitcoin's popularity has risen rapidly since 2016,[11] so the number is certainly larger now. The distribution is global, but all members of the community have similar values, or else they would not use Bitcoin. All care about using a decentralized currency for one reason or another, mostly to avoid state influence, and many of them care about earning Bitcoin the 'right' way, without cheating.[12] They all believe that their participation will result in financial gain, or else they would not participate. Participants skew young, male, and nerdy.[13] They all share roughly the same set of data points: the current price and production rate, along with past trends. Miners know the cost to produce a Bitcoin, and only participate if it continues to be profitable. Users and intermediaries know the current exchange rate and transaction fees, and similarly would not participate if these made participation unprofitable. Community members'

---

[8] Nadeem, "If We Lived in a Bitcoin Future, How Big Would the Blockchain Have to Be?"
[9] Gencer and Sirer, "State of the Bitcoin Network."
[10] Donet, Pérez-Sola, and Herrera-Joancomartí, "The Bitcoin P2P Network," 1.
[11] "Total Number of Transactions."
[12] Bohr and Bashir, "Who Uses Bitcoin? An Exploration of the Bitcoin Community," 96–97.
[13] Comben, "Google Analytics Reveal Surprising Bitcoin Demographics."

specific beliefs about the preferences of other participants are largely irrelevant, since they would simply opt out of the system if they held deep suspicions about other participants.

Rules-in-Use

The rules-in-use of the Bitcoin community are not complex. For the purposes of this essay, three roles exist for participants to fill: miner, payment intermediary, and user. The boundary rules for each are straightforward: to become a miner, one must run the mining algorithm on a computer with a network connection; to become an intermediary, one must set up methods for exchanging Bitcoin for other forms of currency; and to become a user, one must acquire Bitcoin. Similarly, the authority rules are simple. Miners can decide to mine or not mine, depending on their incentives, and they can approve or decline proposed additions to the blockchain. Payment intermediaries can set exchange rates between Bitcoin and other currencies on their platforms. Users can buy and sell Bitcoin through the methods of their choice. The major aggregation rule involves miners using the Nakamoto consensus algorithm to approve or decline new blocks.[14] The effective scope rule is that actions taken by community members can only affect the rate of Bitcoin production, and in some cases the exchange rate. Because of the decentralized nature of the blockchain, essentially all information is available to all participants if they want it, although users likely do not possess all of this information. Finally, there are four main payoff rules. Users get Bitcoin through intermediaries if they pay the correct amount. Miners get a Bitcoin payoff if they mine a valid block,[15] and they also get a Bitcoin payoff if

---

[14] Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 3.
[15] Nakamoto, 4.

they put other participants' transactions in their block.[16] Last, miners in pools receive proportional payoffs to the amount of computing power that they contribute to the pool.[17]

Integrating the Analysis

The participants in the Bitcoin system are a geographically diverse but demographically homogenous group. They are able to take individual-level actions that affect their personal outcomes, but individual participants possess little power to affect the system as a whole. As previously mentioned, participants are mostly young male nerds,[18] and they can hold the roles of miner, intermediary, or user. Miners can choose to mine if the price of Bitcoin justifies their expenses, though each miner's participation decreases the proportional rewards to all miners. Intermediaries can choose the exchange rate between Bitcoin and other currencies on their platforms, which affects the perceived market value of Bitcoin. Users can choose to buy or sell Bitcoin, which influences the exchange rate and market value just as market activity in the stock market affects stock prices. Notably, each participant's choices do not have large effects on the broader Bitcoin system, but rather their collective choices—which may be driven by the same factors—drive changes in the system.

Patterns of Interaction

The structure of economic and political participation is decentralized and market-driven. Political participation happens through the Nakamoto consensus protocol, although mining pools can have internal rules that institute additional methods of political participation. Economic

[16] "Bitcoin Network Fees: Everything You Need to Know."
[17] Eyal, "The Miner's Dilemma," 1.
[18] Comben, "Google Analytics Reveal Surprising Bitcoin Demographics."

participation for users happens when they buy or sell Bitcoin through intermediaries, and intermediaries can set prices wherever they see fit, subject to market pressures. Miners expend real money in the form of electricity and computer costs, and receive per-block rewards in return. The Bitcoin network is also an economic actor, automatically setting the hash difficulty depending on the rate of production.[19]

The main information flow in Bitcoin deals with the proposal and acceptance of new blocks. A miner proposes a new block to add to the blockchain, sending it to the network of other miners that can accept or reject the block.[20] If more than half of the computing power in the network accepts the block, it becomes part of the blockchain, and most participants treat a block as confirmed once it is six blocks deep. Another information flow is the buying and selling of Bitcoin through intermediaries: intermediaries know the going market rates and set prices, and users can decide to buy or sell according to those rates.

Outcomes

The current system outcomes fulfill some of Ostrom's evaluative criteria. It achieves economic efficiency for miners' immediate costs, or else they would not choose to mine Bitcoin. However, once environmental externalities[21] enter the equation, economic efficiency falters. Similarly, the system achieves fiscal equivalence for miners but fails to internalize the environmental impacts of mining. Bitcoin does not achieve distributional equity, since the price is constant for all participants. The system is very accountable thanks to the Nakamoto consensus protocol: all miners have access to information at low cost, hash functions make evaluation

---

[19] Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 3.
[20] Nakamoto, 3.
[21] Temple, "Bitcoin Mining May Be Pumping out as Much CO2 per Year as Kansas City."

straightforward, and miners can easily enforce sanctions by rejecting bad blocks. The system conforms to general morality reasonably well, since a potential attacker would have to control more than half of the computing power in the network in order to create unfavorable outcomes. Lastly, the system is adaptable, since it frequently adjusts the hash difficulty, but it is not sustainable, because of the environmental impacts of mining.[22]

Ostrom's Principles

Elinor Ostrom analyzed thousands of common-pool resource appropriation situations using the IAD framework,[23] much like the analysis presented above. From these analyses, she constructed a set of eight design principles that tend to characterize sustainable resource appropriation. Ostrom notes that not all sustainable systems fulfill all eight design principles, but that successful systems tend to fulfill more of them than unsuccessful systems.[24] This section will analyze the Bitcoin system's fulfillment of these principles, providing policy recommendations where it falls short if possible.

Ostrom's first design principle is "clearly defined boundaries,"[25] and Bitcoin somewhat fulfills this. The boundary condition for becoming a miner is clear—whether or not someone mines Bitcoin—and similarly, payment intermediaries must run a platform for buying and selling Bitcoin in order to become part of the group of intermediaries. The boundary condition for users asks whether someone owns any Bitcoin through an intermediary, but this means that people can participate without becoming a part of the Bitcoin community. This becomes a problem when linked with the issue of Bitcoin as an investment vehicle: when people can buy and sell Bitcoin

---

[22] Temple.
[23] Ostrom, *Governing the Commons*, xiii.
[24] Ostrom, 90–91.
[25] Ostrom, 90.

without a meaningful stake in its future stability, volatility can increase dramatically. I see no clear policy fix for this. Bitcoin's accessibility through payment intermediaries helped it gain widespread adoption, and far fewer people would likely participate if forced to become part of the community in order to own Bitcoin. For example, banning payment intermediaries and requiring all users to mine would substantially shrink the number of users, given the technical complexity of mining. Although Bitcoin somewhat fulfills Ostrom's first principle, no clear policy solution exists to encourage Bitcoin to completely fulfill it.

Bitcoin does not fulfill Ostrom's second design principle: "congruence between appropriation and provision rules and local conditions."[26] The rules of Bitcoin appropriation are constant everywhere, meaning that they do not adapt to locations with less computing power or more expensive electricity costs. This privileges certain areas that may or may not have greater need for Bitcoin. I do not believe that a system-wide policy solution for this would be tenable, given how much it would complicate the system. Take the hypothetical solution of easing the hash difficulty in places with less computing power or more expensive electricity: first, how would the Bitcoin system implement this? Implementation alone probably precludes this from happening, and especially when one considers how this would set up a system ripe for exploitation by opportunistic miners, it seems unlikely at best. Mining pools with expanded influence could enact solutions, a possibility explored later in this paper, but system-wide policy solutions do not seem promising.

Ostrom's third design principle, "collective-choice arrangements" that enable those affected by the rules to change the rules,[27] is somewhat fulfilled by Bitcoin. Modifying Bitcoin's

---

[26] Ostrom, 90.
[27] Ostrom, 90.

rules is possible, but only with network consensus in agreement with the new rules.[28] This means that minor tweaks can be difficult, but issues affecting all miners (or a majority, at least) can be fixed. However, issues that disproportionately affect a minority of miners may not be resolved, particularly if they benefit a majority at the expense of a minority. In this case, forking represents the minority's only real option short of ending their participation in Bitcoin, but forks hurt everyone involved and do not represent an optimal solution. Pools probably represent the best potential solution to this problem, giving minority voices a platform to gain some form of recourse, but the full Bitcoin system by design cannot do this.

Bitcoin fulfills Ostrom's fourth design principle: "monitoring" by community members of other members' behavior.[29] Looking at behavior in the sense of correctness of published blocks and transactions, the Nakamoto consensus protocol functions as a version of this principle running as code, punishing bad behavior by rejecting incorrect blocks and transactions. All 'good' actors have an incentive to call out 'bad' behavior in this sense, since they have an economic stake in the continuing correctness and validity of the blockchain. This works as long as 'good' actors control more than half of the mining power, and overall, Nakamoto consensus fulfills Ostrom's fifth guideline.

Bitcoin implicitly fulfills Ostrom's fifth guideline: "graduated sanctions" for rule violators.[30] For the violation of proposing bad blocks, graduated sanctions are natural, since more time spent mining and proposing bad blocks corresponds to less rewards from mining good blocks. As mentioned above, this requires that 'good' actors control more than half of the mining power, but the system currently works.

---

[28] "Frequently Asked Questions."
[29] Ostrom, *Governing the Commons*, 90.
[30] Ostrom, 90.

Ostrom's sixth guideline, low-cost "conflict-resolution mechanisms,"[31] is not fulfilled for individual actors in the Bitcoin system. If an individual has an issue, the only real method of recourse that they have is to stop participating in the system. Small groups, as mentioned above, can fork if they have been harmed by a larger group, but this is costly for the small group. Similar to other solutions mentioned above, pools represent a possible avenue for meaningful policy solutions, but for now, Bitcoin does not fulfill Ostrom's seventh guideline.

At the federal level in the United States, Bitcoin fails to fulfill Ostrom's seventh design principle: "minimal recognition of rights to organize" by outside authorities.[32] Some states have passed legislation encouraging Bitcoin usage,[33] but the federal government's attempts at regulating Bitcoin have not displayed recognition of the Bitcoin community's ability to self-govern.[34] In fact, given the federal government's suspicion of Bitcoin as a platform for illicit activity,[35] the opposite seems to happen.[36] The policy fix for this issue is clear and straightforward—the federal government would have to pass legislation affirming the Bitcoin community's right to self-determination—but appears unlikely any time soon.

Lastly, although Bitcoin does not fulfill Ostrom's eighth guideline of "nested enterprise,"[37] pools could represent a policy solution for this guideline and others, as mentioned above. Pools currently function as economic alliances, serving to stabilize income for participating miners. In the future, they could adopt internal policies to better serve their participants, and well-designed policies could solve many of the issues outlined above,

---

[31] Ostrom, 90.
[32] Ostrom, 90.
[33] Vigna, "Pay Taxes With Bitcoin? Ohio Says Sure."
[34] Romm, "Bitcoin Could Face New Regulations in the U.S. after Top Financial Cops and Lawmakers Raise New Fears about Virtual Currency."
[35] Huddleston Jr., "This Ohio Man Is Accused of Trying to Launder $19 Million of Bitcoin from the Dark Web."
[36] Cox, "Treasury Secretary Mnuchin Wants to Keep Cryptocurrencies Away from 'Bad Guys.'"
[37] Ostrom, *Governing the Commons*, 90.

particularly those that deal with potential tyranny of a majority. This would represent a departure from the current structure of Bitcoin and pools, but would also constitute substantial progress towards satisfying Ostrom's eighth guideline, and probably others.

Policy Solutions

What policies could Bitcoin adopt in order to fulfill more of Ostrom's principles? As an outside observer of Bitcoin and mining pools, take these recommendations with a grain of salt, but here are my ideas. I believe that any meaningful change would have to come through pools, rather than the entire system. Reform of the entire system seems incredibly unlikely, and also technically difficult—pools represent a smaller and more flexible unit of governance. As far as pool reform goes, first and foremost, pools need constitutions that lay out political and economic rights. These do not have to be as sweeping as the American constitution, but they need to contain rules that pool members agree upon, particularly around reward structures, mechanisms for dispute resolution, and amendments to the rules. Ostrom's second principle could be satisfied by some sort of reward structure that took into account the computing power and electricity costs of each miner, though some miners would undoubtedly support this more than others. Her third and sixth principles could be fulfilled by an equitable amendment and dispute resolution process that took into account the degree of harm, instead of just the number of users affected. Lastly, the existence of more political pools would fulfill Ostrom's eighth design principle, especially if pools start featuring 'sub-pools,' which seem to be a natural extension of the policy changes presented here.

Conclusion

Overall, Bitcoin shows some promise for fulfilling more of Ostrom's design principles, but the currency's future compliance with the principles appears to rest on whether mining pools can become political bodies, in addition to their current economic function. In doing so, they would begin to further resemble other common-pool resource appropriation communities, which are commonly tight-knit and socially close. Whether this is possible over the internet remains an open question, as these other communities are often small, remote towns,[38] so strong community comes naturally. Members of Bitcoin mining pools will likely never meet one another in person, but instead will have to trust their political representation and economic futures to strangers on the other side of the world.

Their ability to do so may determine the future existence of Bitcoin and similar cryptocurrencies. Decentralized cryptocurrencies represent a fundamentally different vision of the global economy than the vision offered by too-big-to-fail banks, and no matter which model one prefers, the continued existence of alternatives to mainstream ideas is critical to the health of democracy. Many people do not trust institutions in today's world, and decentralized cryptocurrencies spark conversations around what an alternative world could look like. If only for this reason, a healthy Bitcoin ecosystem, hopefully enhanced by adherence to Ostrom's design principles, should continue to exist.

[38] Acheson, *Capturing the Commons*, 35.

Works Cited

Acheson, James M. *Capturing the Commons: Devising Institutions to Manage the Maine Lobster Industry*. Hanover, NH: University Press of New England, 2003. http://site.ebrary.com/id/10989754.

AtomicWallet.io. "Bitcoin Network Fees: Everything You Need to Know," September 9, 2019. https://atomicwallet.io/bitcoin-network-fees.

Bohr, Jeremiah, and Masooda Bashir. "Who Uses Bitcoin? An Exploration of the Bitcoin Community," 94–101, 2014.

Comben, Christina. "Google Analytics Reveal Surprising Bitcoin Demographics." *Bitcoinist* (blog), June 26, 2019. https://bitcoinist.com/google-analytics-bitcoin-demographics/.

Cox, Jeff. "Treasury Secretary Mnuchin Wants to Keep Cryptocurrencies Away from 'Bad Guys.'" *CNBC*, January 30, 2018. https://www.cnbc.com/2018/01/30/treasury-secretary-mnuchin-keep-cryptocurrencies-from-bad-guys.html.

Donet, Joan Antoni Donet, Cristina Pérez-Sola, and Jordi Herrera-Joancomartí. "The Bitcoin P2P Network," 87–102. Berlin, 2014.

Eyal, Ittay. "The Miner's Dilemma." Cornell University. Accessed December 13, 2019. https://www.cs.cornell.edu/~ie53/publications/btcPoolsSP15.pdf.

bitcoin.org. "Frequently Asked Questions." Accessed December 13, 2019. https://bitcoin.org/en/faq#could-users-collude-against-bitcoin.

Gencer, Adam Efe, and Emin Gün Sirer. "State of the Bitcoin Network." *Hacking, Distributed* (blog), February 15, 2017. http://hackingdistributed.com/2017/02/15/state-of-the-bitcoin-network/.

Hardin, Garrett. "The Tragedy of the Commons." *Science* 162, no. 3859 (December 13, 1968): 1243–48. https://doi.org/10.1126/science.162.3859.1243.

Huddleston Jr., Tom. "This Ohio Man Is Accused of Trying to Launder $19 Million of Bitcoin from the Dark Web." *CNBC*, July 23, 2019. https://www.cnbc.com/2019/07/23/man-accused-of-laundering-millions-in-bitcoin-from-silk-road.html.

Morell, Mayo Fuster. "Governance of Online Creation Communities: Provision of Infrastructure for the Building of Digital Commons." Louvain-la-Neuve, Belgium, 2012. http://hdl.handle.net/10535/9564.

Nadeem, Subhan. "If We Lived in a Bitcoin Future, How Big Would the Blockchain Have to Be?" *HackerNoon* (blog), December 4, 2017. https://hackernoon.com/if-we-lived-in-a-bitcoin-future-how-big-would-the-blockchain-have-to-be-bd07b282416f.

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System," n.d.

Ostrom, Elinor. *Governing the Commons: The Evolution of Institutions for Collective Action*. Canto Classics. Cambridge, United Kingdom: Cambridge Univ Press, 2015.

Polski, Margaret M., and Elinor Ostrom. "An Institutional Framework for Policy Analysis and Design," June 15, 1999.

Romm, Tony. "Bitcoin Could Face New Regulations in the U.S. after Top Financial Cops and Lawmakers Raise New Fears about Virtual Currency." *Vox*, February 6, 2018. https://www.vox.com/2018/2/6/16979498/bitcoin-regulation-sec-cftc-congress.

Shackelford, Scott J. "Governing the Internet of Everything." Indiana University, Bloomington, 2019. http://hdl.handle.net/10535/10533.

Temple, James. "Bitcoin Mining May Be Pumping out as Much CO2 per Year as Kansas City." *MIT Technology Review* (blog), June 12, 2019.

https://www.technologyreview.com/s/613658/bitcoin-mining-may-be-pumping-out-as-much-cosub2-sub-per-year-as-kansas-city/.

Blockchain.com. "Total Number of Transactions." Accessed December 13, 2019. https://www.blockchain.com/charts/n-transactions-total?timespan=all.

Vigna, Paul. "Pay Taxes With Bitcoin? Ohio Says Sure." *Wall Street Journal*, November 26, 2018. https://www.wsj.com/articles/pay-taxes-with-bitcoin-ohio-says-sure-1543161720.