Received: 19 July 2021 | Accepted: 2 September 2021

DOI: 10.1111/phc3.12784

ARTICLE

WILEY

Philosophy, politics, and economics of cryptocurrency II: The moral landscape of monetary design

Andrew M. Bailey[1] | **Bradley Rettler**[2] | **Craig Warmke**[3]

[1]Division of Humanities, Yale-NUS College, Singapore, Singapore

[2]Department of Philosophy, University of Wyoming, Laramie, Wyoming, USA

[3]Department of Philosophy, Northern Illinois University, DeKalb, Illinois, USA

Correspondence
Andrew M. Bailey, Division of Humanities, Yale-NUS College, Singapore, Singapore.
Email: wrathius@gmail.com

Abstract

In this article, we identify three key design dimensions along which cryptocurrencies differ – privacy, censorship-resistance, and consensus procedure. Each raises important normative issues. Our discussion uncovers new ways to approach the question of whether Bitcoin or other cryptocurrencies *should* be used as money, and new avenues for developing a positive answer to that question. A guiding theme is that progress here requires a mixed approach that integrates philosophical tools with the purely technical results of disciplines like computer science and economics.

1 | INTRODUCTION

In a companion article, we distinguish descriptive, empirical, or technical questions about cryptocurrency's status as money from normative questions about whether a given cryptocurrency *should* be used as money. One way to approach such normative inquiry is to identify dimensions along which cryptocurrencies differ and show their moral upshots:

> *Monetary Policy*. Cryptocurrencies differ in their inflation rates, total future supplies, the amount and nature of their supplies at their network's genesis, and the introduction and distribution of future supplies.
> *Privacy*. Some privacy-focused cryptocurrencies allow for shielded or private transactions where the sender, the receiving address, or the amount are hidden from view. Others offer privacy through obscurity within a crowd.
> *Censorship-Resistance*. How easy is it to contribute to the network or transact over it? Who, if anyone, gives permission to do so? Can anyone block transactions?
> *Consensus*. Some networks use something other than solving math problems to update the ledger. What do they use, and what are the tradeoffs?

Having addressed monetary policy in our companion article, we dedicate the remainder of this article to the last three – privacy, censorship-resistance, and consensus.

2 | PRIVACY

Someone enjoys privacy to the extent that others have limited access to her personal information and personal space.[1] We need not precisely settle just what kinds of information or space count as "personal", but we will assume that financial information – information about wealth, income, buying, selling, and so on – qualifies as personal.[2]

Privacy has seemed to many a *pro tanto* good that makes us better off in some respects.[3] Although privacy is also seemingly a final good – a good properly valued for its own sake – it also has instrumental value in enabling social relationships, contributing to human dignity, and facilitating variety in lifestyle.[4] This can all be true, note, even if privacy makes us worse off in other respects, and even if we have no absolute right to privacy.[5] Despite widespread agreement on the value of privacy, financial privacy – that is, privacy with respect to buying, selling, and storing value – is not widely discussed or defended. As we'll see, though, it deserves renewed attention, especially in relation to cryptocurrencies. For as financial privacy continues to erode, cryptocurrencies provide new tools to protect it.

2.1 | Financial privacy under threat

Many factors contribute to declining financial privacy: a rise in corporate and state surveillance capacity, the rise of credit and corresponding decline of physical cash for everyday consumer transactions, big data, and so on.[6] More eyes vie for personal financial information with fewer checks on the power to acquire it.[7] Private corporations now collect, analyze, trade, and act on huge swaths of personal financial data, resulting in a "surveillance capitalism" that should concern those indifferent to government surveillance.[8] Something valuable seems under systematic threat.

We face an uneasy dilemma between convenience and privacy. We could stick to the convenience of things like credit cards and cede financial privacy.[9] Or we could renounce these conveniences for privacy-enhancing physical cash. In doing so, we would relinquish faster and simpler payment tools, access to credit, and other financial instruments. Perhaps cryptocurrencies could offer a third way of convenient yet private payments.

2.2 | Solutions

We begin with Bitcoin, which does not automatically provide users with significant financial privacy.[10] The Bitcoin ledger is public and all amounts, destinations, and sources are available for inspection by all. To be sure, the Bitcoin ledger itself does not connect its pseudonymous addresses with real-world identities like legal names, phone numbers, birth dates, and so on. But with enough resources, state and corporate entities can and do draw these connections, especially since regulated exchanges require customers to provide identifying information.[11]

One can, however, transact with Bitcoin more privately. In a CoinJoin transaction, multiple people use a single transaction to send value back to themselves at new addresses, severing their identities from the bitcoin held at their old addresses. Furthermore, since a Bitcoin transaction's inputs don't map explicitly to any given output, the transaction histories of the Bitcoin entering a CoinJoin get smeared across every quantity of Bitcoin exiting the transaction.[12] All transactions remain public, but the ledger doesn't say whether the transaction is a true CoinJoin involving many people, or just some random user sending Bitcoin from old addresses to new ones.[13] So even if we had known who had which Bitcoin at which addresses going in, we wouldn't know who received how much Bitcoin on the other end.[14]

One could also use a cryptocurrency with better built-in privacy options.[15] These options provide two methods for resisting surveillance: *shielding* and *obscurity*.[16] Privacy through obscurity provides anonymity within a group.[17] Obscured transactions drive a wedge between users' real-life identities and the ledger's fully visible financial details. CoinJoin is an example of privacy through obscurity. Another obscuring strategy – implemented by Monero – deploys *ring signatures*. Whereas each Bitcoin transaction determinately claims one or more sources of Bitcoin within a trans-

action, a Monero transaction involves a ring of possible sources. Only the originating user knows which member of the ring is the true source. Under best practices, no one else can tell.

By shielding, we mean cryptographically secured secrecy. A shielded transaction uses a kind of mathematical armor that prevents third parties from unveiling its financial details. Perhaps the most well-known shielding strategy involves *zero-knowledge proofs*.[18] In a system with zero-knowledge proofs, like Zcash, users can send and receive value on a public ledger without revealing any information about amounts, destinations, or sources.[19]

Financial privacy achieved through either shielding or obscurity benefits from network effects. The more transactions processed in either way, the stronger their privacy.[20] This holds especially for privacy through obscurity. The bigger swarm of indistinguishable transactions (or participants in a ring signature), the more privacy each enjoys. But these swarms raise important questions. Users who participate, whether as miners or transactors, do not merely secure privacy for themselves – they secure it for others, too – both the noble and the nefarious.[21] Should this worry them? Perhaps not; double-effect reasoning may apply here. Roughly, subjects avoid moral responsibility for the foreseeable consequences of an action provided that they do not intend those consequences, like helping bad actors conceal their activities.[22] Ordinary consequentialism could also apply here as we weigh the benefits and drawbacks of financial privacy.

In sum, cryptocurrencies can promote financial privacy. Therefore, cryptocurrencies exemplify an important instrumental value. A more thorough evaluation would require weighing the goods that cryptocurrencies promote against those that they thwart.[23] But we have uncovered one path for the claim that cryptocurrencies should be used as money: *yes, it is good to use cryptocurrency as money because doing so promotes privacy*.

And one can affirm this without taking privacy to be a final good. Privacy may instead be good only because it is instrumental in promoting other goods. First, privacy can help users resist unjust state and corporate censorship. It's hard to censor what you can't find. Second, increased privacy promotes increased fungibility. A money with a more private history is a money that's more easily interchangeable. And something's fungibility helps it play key money roles. It's interesting, then, that the very privacy-enhancing features of cryptocurrencies that distinguish them from traditional forms of money could simultaneously help them fulfill traditional money roles.

3 | CENSORSHIP-RESISTANCE

We've noted that the ubiquity of cashless transactions erodes financial privacy. Cashless transactions come with another drawback: many of those who sit atop financial superhighways and track our purchases also have the power to prevent them. Cryptocurrencies can protect against more than just state or corporate intrusion into our financial lives; they can also protect against state and corporate control over who gets to buy what, when, and from whom. We'll argue that the permissionless architecture towards which cryptocurrencies aim limits the capacity of corporations and states to control our economic behavior. Many here contrast *centralized* from *decentralized* payment networks, with Bitcoin and other cryptocurrencies given as examples of the latter. We prefer to speak of the degree to which a network requires permission to join or use. One reason we're wary of decentralization talk is that Bitcoin and other cryptocurrencies are to some degree and in some ways centralized.[24]

We'll first describe how state and corporate entities presently control who has access to financial systems.

3.1 | Permissioned payments

We increasingly transact by sending digitized information through multiple parties on a payment network.[25] The more visible parties provide consumers gateways to the network with cards and software applications to initiate transactions. Less visible parties – for example intermediary banks and clearinghouses – authorize, clear, and settle those transactions.[26]

We'll call a party on a payment network an *authority* when it can reliably block transactions on the network.[27] Authorities can block differently depending on where they perch along the financial superhighway. Entry points like Venmo may deny you access. Intermediaries like Wells Fargo may block particular transactions, certain kinds of transactions, transactions with certain people or companies, or deny you service entirely. While most authorities can prevent transactions from taking one *particular* path through a network, they usually can't stop transactions from taking a detour through other authorities. However, an unavoidable hub in a payment network – like a central bank – can block someone from using a network altogether.

An authority may have a group-centered, entity-centered, or transaction-centered approach to blocking. In group-centered blocking, authorities block transactions from those with a certain feature, like a political affiliation, religious commitment, career, or level of credit. In entity-centered blocking, authorities might block transactions from a particular person or organization, like the outspoken whistleblower or the non-profit watchdog. And instead of blocking all transactions from particular people or organizations, an authority might block certain kinds of transactions, like transactions involving drugs, pornography, or copyright infringement.[28]

Since authorities can block transactions on the network, we need their permission to transact. We ask for permission initially when we open accounts at our local banks, apply for credit cards, or accept the Terms of Service agreement with an electronic payments provider. But authorities can revoke permission at any time. Every single attempted transaction will fail unless authorities grant it permission and usher it through their location on the payment network. Given this connection between authority and permission, we call a payment network *permissioned* when it has one or more authorities.

Transaction settlement over a payment network requires transmitting information about such things as the payer, the payee, and the amount paid. Because authorities on permissioned networks control the flow of this information, they can block certain kinds of transactions or transactions from or to certain entities. They can also abuse their power to extract fees – perhaps unjust ones. Authorities have abused their power in each of these ways, and their doing so amounts to an underexplored kind of censorship – financial censorship.

3.2 | Financial censorship illustrated

Permissioned networks are vulnerable to financial censorship. We may benefit from reviewing some cases of financial censorship:

Marijuana. Some US states permit the sale of marijuana, but dispensaries in these states deal in cash. Why? The federal government still forbids the sale of marijuana. Since other forms of payment rely on banks, which, in turn, use the federal reserve payment system, banks cannot serve marijuana dispensaries without risking stiff penalties and the loss of FDIC insurance.[29]

Sex. Corporate payment processors censor transactions to protect their reputations or stave off regulatory intervention. In 2012, Paypal pressured the indie publisher Smashwords to stop selling books with adult content.[30] In 2014, JPMorgan Chase terminated the accounts of many involved in the adult film industry.[31] This came on the heels of Chase refusing to process payments for Lovability, an online condom store.[32] And, in 2017, the adult social network FetLife saw its payment services revoked.[33]

Remittances. Cross-border payments often involve migrants sending money home in payments routed through fee-extracting authorities. Globally, the average remittance fee is about seven percent for a US $200 payment. But depending on the locations of the sender and the recipient, the fees can climb much higher; the average remittance fee to send US $200 from South Africa to Botswana, for example, exceeds 19%.[34] Expensive remittances arguably count as a form of financial censorship because authorities block, and collect, a higher than necessary percentage of the amount intended for the recipient.

These cases are by no means unique to the US:

> *Russian Political Dissent*. Opposition activists and politicians in Russia need money to organize and campaign for political change. But conventional channels for securing funds are closed off or made costly through fines, legal harassment, frozen bank accounts, and so on.[35]
> *Social Credit in China*. The two dominant payment applications in China, WeChat and AliPay, together have around 2 billion users. Since Chinese internet companies must share data with the Chinese Communist Party by law, these corporations double as arms of China's vast surveillance state.[36] Transaction data figure into "social credit" scores that reflect an individual's overall reputation. These scores not only chill speech and restrict movement of those deemed "untrustworthy" but incentivize others to sever contact with them. As of July 2019, over 13 million individuals appeared on a blacklist that prevents them from flying (over 20 million flights blocked), buying high-speed train tickets, and sending their children to private schools.[37]

3.3 | Financial censorship is dangerous

At least some of these cases will trouble many. Still, some may resist the overall point here on the grounds that we must weigh the abuses of permissioned networks against the goods they enable, such as preventing transactions involved in illegal drugs, money laundering, terrorism, copyright infringement, and, more globally, efforts to avoid economic sanctions. But although some may cheer at the financial censorship of unpopular but law-abiding entities, history suggests that it won't be long before the shoe is on the other foot.[38] The power to block illegal transactions is also the power to block legal transactions, as well as illegal but morally praiseworthy ones.

Some authorities are private and may be said to have a legal right to restrict use or access. This legal right and the private nature of the authorities in question doesn't imply that their exercise of authority is beyond reproach. We'll argue the point in three ways.

First, comparison to the phenomenon of employer overreach is instructive. It is no secret that large firms increasingly exercise unprecedented and pervasive control over employees, both on and off the clock.[39] There is something deeply concerning here. Human well-being is simply not promoted by such employer meddling, even if the employment is voluntary. Similarly, observing that some sources of financial censorship are private doesn't mean they do no harm or that we oughtn't look for ways around the censorship. Private censorship may not be as coercive as state censorship, but it may nonetheless be harmful.

Second, since large firms are often enmeshed with the state, discerning "private" from "state" censorship isn't always easy. Indeed, private firms often have little choice but to engage in financial censorship at the direction of a state.[40] States sometimes pressure private authorities domiciled within their boundaries to engage in financial censorship, whether directly by law or by less direct means. And since states themselves are party to payment networks both inside and outside their national borders, they can also censor economic behavior both at home and abroad.[41]

Third, private censorship – whether of speech or of financial activity – exhibits some of the same troubling biases and trends that make state-sponsored censorship worrisome. So Tusikov:

> A growing body of scholarship shows private actors' policing of speech disproportionately affects marginalized or vulnerable actors engaging in controversial or critical speech but not violent speech… platforms' regulatory efforts often have weak due-process mechanisms, lack transparency and accountability measures, and can disproportionately stifle the speech of marginalized populations.[42]

So we think that financial authorities exercise an objectionable degree of control. The root condition is structural and holds across both state and private actors: traditional payment networks rely on trusted and central intermedi-

aries.[43] Banks, states, credit agencies, and so on have the power to censor transactions between two parties because they stand between those parties.

The question isn't whether we should have any permissioned networks at all. The question is whether we should have permissioned networks alone. We claim that having an alternative would be desirable, especially given the abuses of financial censorship in less free and prosperous parts of the world.

3.4 | Permissionless payments

Where might we look for alternatives? One might look for public policy solutions. But for them to work, powerful authorities around the world would have to cede their perches atop the global financial system – this applies to both governments and corporations.[44] They're likely to resist.

Cryptocurrencies like Bitcoin inhabit payment networks built to lack authorities, and traditional institutions have thus far been unable to stop them due to their distributed networks. They aim to be *permissionless*.[45] And the more private cryptocurrencies offer another level of protection against censorious authorities. With shielding and obscurity protections in place, states and firms cannot effectively track individual users or particular transactions. So cryptocurrencies tempt these institutions to issue bans on entire networks that, due to matters of politics of practical computer science, likely cannot succeed and which thereby further highlight the fundamental value of those networks.[46]

Although several cryptocurrency networks remain highly centralized and permissioned, the Bitcoin network in particular has achieved a relatively high degree of permissionlessness. We do not say, as many do, that cryptocurrencies are trustless. Whereas our trust in permissioned networks should pool around their authorities, one's trust in a strongly permissionless network spreads more thinly over the network itself.[47]

A network like Bitcoin achieves strong permissionlessness in several ways. The software is open-source and anyone can inspect it. No registration is required to join. And with the internet and a free, open-source application, anyone may construct a transaction and send it to the network. But the permissionlessness of many cryptocurrencies extends beyond the realm of sending and receiving value. In Bitcoin and other cryptocurrencies, users together play the roles of banks and clearinghouses. Without authorities, the network as a whole validates, settles, and clears transactions. With nothing but internet access and free, open-source software, anyone may join the network to validate, settle, and clear transactions – including one's own.

3.5 | Financial inclusion beyond payments

Many suffer for lack of adequate credit and banking, often at the hands of financial authorities. Just as cryptocurrency networks can help some route around unjust authorities for payments, perhaps those same networks can offer more just forms of credit and banking.

Credit is a vital avenue to wealth creation. But unfair obstacles prevent some from getting credit. For example, through redlining, the U.S. Federal Housing Administration refused to insure mortgage loans to people living in color-coded neighborhoods – primarily lower-income Black people living in urban areas. Effects of this are still seen today, where Black families comprise 13% of the population but own 1% of the wealth in the U.S.[48] Exclusion from credit markets is economically devastating, so unsurprisingly, people seek credit elsewhere. Each year 12 million Americans take out a payday or car title loan. The average loan is $375, but the average loanee pays $520 in interest.[49]

Many also suffer from poor access to banking. 22% of U.S. households remain unbanked, often because they fail to meet minimum balance requirements. Without access to traditional instruments, the unbanked routinely pay for things like prepaid debit cards, money orders, and cashing paychecks.[50] The average unbanked family pays 10% of its income, or $2400 a year, on financial transactions like these. In total, the unbanked pay approximately $89 billion per year in transaction fees.[51]

The poor, then, suffer without access to borrowing and banking. The problems here, we emphasize, are not merely practical; they involve inequities and injustice.[52] A monetary system that offers banking or credit only to some is unlikely to pass important tests for fairness or justice.

Cryptocurrency promises to mitigate both problems.[53] Unlike bank accounts, cryptocurrency addresses require neither permission nor minimum balances. Compared to banks, several cryptocurrency banks and lending platforms offer a much higher yield on savings, as high as 6 - 12%, even on so-called "stablecoins" that track the values of fiat currencies. And unlike traditional lenders, a number of cryptocurrency lending platforms offer credit to users without so much as a name, much less bias-inducing information about race or neighborhood. Anyone with enough collateral in cryptocurrency can receive a loan.[54]

In summary, cryptocurrencies democratize monetary value in much the same way the internet has democratized information. While the internet provides a difficult-to-censor pathway for valuable information, cryptocurrencies provide a difficult-to-censor pathway for monetary value itself. And as the internet has mitigated the effects of book bans and other attempts to censor information, so cryptocurrencies mitigate the effects of payment blockades and other forms of financial censorship.[55]

The internet has enabled new modes of wrongdoing, to be sure. But many would accept these as costs outweighed by greater goods. The internet contributes to human flourishing and the development of free and open societies.[56] Similarly, although we recognize the new modes of wrongdoing cryptocurrencies enable, we expect the benefits of cryptocurrencies to outweigh their costs. Since Bitcoin and other cryptocurrency networks serve as a censorship-resistant payment system, many around the globe increasingly see them as an exit from and hedge against traditional payment systems.[57] As a result, they may increasingly serve as a competitive check against those systems. And, like the internet, we expect cryptocurrencies to contribute to human flourishing.

4 | CONSENSUS

Traditional electronic monetary networks achieve consensus about who has which amounts of money through trusted authorities who say who has which amounts of money. Should users disagree, they must convince authorities that things have gone awry (as when one disputes a charge or unexpected withdrawal). Cryptocurrencies achieve consensus without trusted authorities. In this section, we discuss how that happens and the tradeoffs of two approaches.

4.1 | Consensus matters

Authorities on payment networks can censor and spy on users precisely because they serve as useful intermediaries. Not only do they settle accounts between parties who may not otherwise trust each other, they also protect the integrity of financial systems by ensuring that no one spends the very same money more than once. We hope it is clear, then, how questions about consensus connect with more familiar normative questions. Since the ledger dictates where the money is, questions about how to update it implicate classic issues in political theory such as *who should rule, and how?* Or *how is the constitution to be amended?*[58] Although cryptocurrencies eschew authorities, they still aim for integrity. Without authorities to issue top-down judgments about who has which amounts of value, cryptocurrency networks must achieve consensus some other way: governance without government.[59]

Bitcoin's approach to consensus – proof of work – has inspired a number of alternatives. Choosing one procedure or another involves tradeoffs. The selection of consensus procedure is, in short, a design choice – and one with normative implications. We'll now explain the two most influential designs, some of their tradeoffs, and some issues at stake.[60]

4.2 | Consensus machines: Work and stake

Updating a ledger without authorities is tricky. Several parties with value at stake have competing interests. You may want the ledger to say that others have recently transmitted amounts to your address, while others would like to keep their amounts right where they are – or even both spend *and* keep them! Coordination without authority has game-theoretic, economic, and political dimensions. There are normative dimensions, too, and we'll highlight a few. As usual, we don't aim to offer decisive considerations but instead hope to provoke further inquiry.

Here are two popular consensus procedures[61]:

Proof of Work (PoW): miners compete to solve a mathematical puzzle that can only be solved by brute force (trial and error). Having provably done *some* computational work and probabilistically a certain amount of it, the winning miner may create the chain's next block.[62]

Proof of Stake (PoS): validators demonstrate stake in a blockchain and the value it stores by, for example, proving that they have control over a sufficiently high amount of the cryptocurrency. The network then picks an eligible validator at random, often weighted to the amount staked, to create the chain's next block.

The jobs of mining in PoW and validating in PoS are, at all times, open to all and, in robust networks, done by many. And miners and validators don't just *say* they've mined or staked; they cryptographically *prove* it – no trust required. We call PoW and PoS "consensus procedures" though neither suffices on its own to reach consensus. To reach network consensus, nodes follow a certain rule about which version of the ledger to adopt. As we've previously mentioned, Bitcoin nodes follow the strongest chain rule and endorse the chain of blocks with the most accumulated proof-of-work.

Both PoW and PoS protect against sybils – cheap internet zombies that could artificially inflate votes for or against a ledger update. In Bitcoin, for example, PoW helps protect against sybils because nodes *must* vote for the chain with the most accumulated proof-of-work. Votes for other chains don't count. The entire procedure is often labeled "Nakamoto consensus" and offers a novel solution to the Byzantine Generals Problem in computer science, a problem about how to achieve consensus without a central authority when something of value is at stake.[63]

PoW and PoS both involve difficult tradeoffs. We'll highlight a few.

Bitcoin deploys PoW,[64] as do Zcash, Bitcoin Cash, Ethereum, and many others.[65] The strongest argument in its favor is its security. PoW requires miners to solve energy-intensive problems, and rewards the first solver with new currency. More energy and better hardware increase the odds of success. PoW guarantees that those who've spent the most on these things have the best chance to win. And those who've spent the most are unlikely to try to cheat the system, since winning honestly is more lucrative than cheating.[66]

However, PoW uses a lot of electricity. A lot. Bitcoin presently uses 0.21% of the world's electricity – about as much as Switzerland.[67] Many find this both wasteful and environmentally harmful. But such criticism may be too quick. To get a sense for whether Bitcoin mining is wasteful or environmentally harmful, we'd need to address questions like:

- How is the electricity produced, and at what opportunity cost?[68]
- How does Bitcoin's use of electricity compare to the resources used by centralized financial institutions to authorize, settle, and clear transactions, implement monetary policy, and protect against counterfeits?[69]
- Does Bitcoin mining encourage more or less harmful ways of producing electricity?[70]

Answers are by no means obvious. So it is unsurprising that some cryptocurrencies forego PoW and deploy alternative consensus procedures instead. Many deploy PoS or variations on it.

PoS assigns the honor of publishing a block to a randomly selected winner; the odds of winning are often proportional to the amount of currency staked and the duration of its staking. The theory is that the more currency you have,

the less likely you are to do something that would potentially devalue it. Suppose you wanted to double-spend some currency. The more currency you have, the more likely you'd be to succeed in publishing blocks with your transactions. But once a double-spend happens, people find out, and the value of the currency (including, obviously, your own amount) likely plummets. The price of security in a PoS model is the opportunity cost of capital; what is staked is not usefully deployed elsewhere.[71]

The primary advantage of PoS is that it is not PoW; it does not, unlike PoW, burn energy for security.

But problems abound.[72] First: the rich get ever richer. The more currency you have, the more likely you are to get more.[73] Although there are technical proposals for limiting this effect, the endgame here tends towards domination by a few early holders.[74]

Second: in PoW currencies, miners choose a network on which to mine and expend resources to mine on that network. Energy is not the only cost here; miners also typically deploy highly specialized hardware that is useful only for mining a given cryptocurrency, for example, ASICs (application-specific integrated circuits) tailor-made for Bitcoin. Having selected a network, miners are unlikely to move to another one – and even if they did, their hardware will still be useful only for mining on that first network.[75] ASICs "anchor" miners to a given network. The incentives here discipline miners away from network-hopping, and in turn motivate convergence. And convergence in turn enhances the network effects of the selected chains in terms of both adoption and security. For PoS currencies, there are fewer disincentives to deploying capital across multiple networks or switching networks regularly in pursuit of profit. There is no analogous anchor for PoS validators on a given network. Staked takens can be easily exchanged for another cryptocurrency and staked on a different network. And so PoS validation can come at the price of robust security assurances into the future and foregoes network effects that make adoption viable.

A final challenge is that PoS simply doesn't have the empirical track record of PoW. The issue here is one of path-dependency. The *present* dominance of Bitcoin's PoW system is in part a function of *past* dominance. And present dominance makes future dominance more likely, even if it could be shown that PoS is superior to PoW in some way.

Consensus without authorities is no easy feat, and the mechanisms by which cryptocurrencies achieve this feat incur serious tradeoffs. How those tradeoffs stack up against each other or against those incurred by legacy systems is an open question and one worth systematic pursuit in future research.

5 | CONCLUSION

If a cryptocurrency *could* fill key money roles, would it be all things considered *good* for it to do so?[76] Two themes have emerged in our discussion. First, there are a range of considerations that support a positive answer. We've argued that cryptocurrencies can promote goods like privacy and financial inclusion – but not without some drawbacks. Second, a responsible treatment of the issues requires a mixed approach that integrates techniques, ideas, and results from philosophy, politics, and economics. Cryptocurrency – and Bitcoin in particular – is a serious topic that deserves more research attention. Academics would do well to pursue it from a variety of angles.

ACKNOWLEDGEMENTS

We thank anonymous referees, the editor, Saifedean Ammous, Alex Arnold, Manka Bajaj, Chris Berg, Jerry Brito, Niaz Chowdhury, Quinn Dupont, Dominic Frisby, Keith Hankins, Jameson Lopp, Peter McCormack, Alaukik Pant, Mike Rea, Kevin Vallier, and Roger Ver for helpful feedback or discussion.

CONFLICT OF INTERESTS

At the time of writing, the authors have modest positions on several of the speculative assets discussed in this article, including USD, BTC, and ETH.

ORCID

Andrew M. Bailey https://orcid.org/0000-0002-6933-0345
Bradley Rettler https://orcid.org/0000-0002-3166-4112
Craig Warmke https://orcid.org/0000-0002-8894-9055

ENDNOTES

[1] This definition loosely follows that in Véliz (2019), p. 149. See also Tavani (2007), Rössler (2005: p. 9ff), DeCew (2018), and van den Hoven et al. (2020). See also the definition given in Hughes (1993): "Privacy is not secrecy. A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world."

[2] See Berg (2018).

[3] There are constitutional protections for privacy across over 20 countries. See also Brooke and Véliz (2020): "1107 people responded to the survey… 82% deemed privacy extremely or very important, and only 1% deemed privacy unimportant."

[4] See Rachels (1975) and Mooradian (2009).

[5] See Moore (2018).

[6] See, for example, Kumar and O'Brien (2019).

[7] See Rahn (1999) for a chilling and prescient expression of this trend.

[8] We borrow "surveillance capitalism" from Zuboff (2019).

[9] See Kahn et al. (2005).

[10] See Reid and Harrigan (2012) and Bohannon (2016).

[11] See Herskind et al. (2020): p. 54,049.

[12] See Warmke (manuscript).

[13] A CoinJoin transaction on the blockchain: https://www.blockchain.com/btc/tx/e4abb15310348edc606e597effc81697bfce4b6de7598347f17c2befd4febf3b.

[14] Biryukov and Tikhomirov (2019): p. 10.

[15] See Blanchette (2012: p. 6).

[16] Compare to Herskind et al. (2020).

[17] See Matthews (2010).

[18] As counter-intuitive as it may seem, zero-knowledge proofs allow a user to prove that a given cryptographic claim is true (that a certain transaction is valid, e.g.) without disclosing its contents. See Li and McMillin (2014) and Androulaki and Karame (2014).

[19] See Herskind et al. (2020).

[20] On privacy through obscurity as a public good, see Kwecka et al. (2014).

[21] On complicity; see Lawson (2013).

[22] Dierksmeier and Seele (2018). On double-effect reasoning, see McIntyre (2019).

[23] Rogoff (2016), especially Chapter 5. Luther (2018) replies to Rogoff. For a defense of the value of privacy, see Swire (1999).

[24] See Walch (2018) and Walch (2019). Luther and Smith (2020): p. 437 argue that Bitcoin is distributed rather than decentralized.

[25] Kumar and O'Brien (2019).

[26] Benson et al. (2017).

[27] Authorities are trusted third parties; see Froomkin (1996).

[28] Bridy (2015).

[29] Baradaran (2020).

[30] Reitman (2012).

[31] Kayyali and Reitman (2014).

[32] Kayyali and Reitman (2014).

[33] Malcolm (2017).

[34] Data from World Bank (2020).

[35] Amnesty (2018).

[36] Wigoder (2019) and McDonell (2019).

[37] Matsakis (2019).

[38] Brito (2019), pp. 20–21.

[39] See Anderson (2017): pp. 39–40.

[40] Kesari et al. (2017): p. 1123 describes Operation Chokepoint.

[41] Kreimer (2006): p. 14.

[42] Tusikov (2019): p. 51 and Noble (2018).

[43] Mann and Belzley (2005): p. 258.

[44] Luther (2020) documents the flaws of cryptocurrency regulations.

[45] On whether Bitcoin makes good on its promise to decentralization, see Gervais et al. (2014).

[46] On cryptocurrency bans, see Hendrickson and Luther (2017) and Hendrickson et al. (2016).

[47] See Maurer et al. (2013): pp. 273–274 and Fama et al. (2019): p. 188.

[48] Black families owned 0.5% of US wealth the year before the Emancipation Proclamation; see Dettling et al. (2017). To be clear, Black wealth is *up*, in both relative and absolute terms; but vast disparities remain. We do not claim that red-lining is the only cause of this disparity, of course. For more on racial disparities here and their origins in access to credit, see Mitchell and Franco (2018) and Rothstein (2018).

[49] Baradaran (2015, 2017) offers extensive evidence of both of these problems and their disproportionate effect on Black communities in the US. See also Flitter (2020) for a recent and lucid account of biased treatment of Black customers by American banks and its effects.

[50] Fraudsters seem to prefer stolen prepaid debit cards over credit cards; see Aliapoulios et al. (2020). As the target market for prepaid debit cards, unbanked individuals bear the brunt of such fraud.

[51] Pew (2012).

[52] On normative issues arising from these inequities, see de Bruin et al. (2020), Sections 4 and 5.

[53] See Rettler (2021).

[54] For an argument to this effect, see Jackson (2019).

[55] Bridy (2015): pp. 1523–1563.

[56] See Nisbet et al. (2012), Ruijgrok (2017), and Stoycheff and Nisbet (2014).

[57] On Bitcoin's censorship-resistance in Russia, see Baydakova (2020).

[58] Though see Pickel (1989).

[59] Cowen (2020).

[60] For the technical and game theoretic issues involved, see Chowdhury (2020): Chapter 3.

[61] For 28 other possible consensus procedures, see Racsko (2019): pp. 358–359.

[62] On PoW blockchains as “trust machines” and the economics governing them, see Berg et al. (2020).

[63] Introduced in Pease et al. (1980) and famously discussed in Lamport et al. (1982).

[64] For details, see Bonneau et al. (2015), p. 4 and Antonopoulos (2015): Chapter 8.

[65] Ethereum developers have promised a move to Proof of Stake since 2015; it remains to be seen whether or how that move will unfold. On the evolution of those promises, see Kim and Edgington (2021).

[66] A point discussed in Section 2.2 of the companion article. See Hasu and Curtis (2019). For skeptical arguments, see Auer (2020) and Budish (2018).

[67] Baraniuk (2019).

[68] Bitcoin is powered to a significant degree by green/renewable energy. See Bendiksen and Gibbons (2019): p. 1, Vincent (2016), Carter (2020), and Harper (2019).

[69] McCook (2014) offers a useful but dated survey of some relevant comparisons.

[70] There may even be positive effects from Bitcoin's energy use. See Bendiksen and Gibbons (2019): p. 10.

[71] See, though, Dale (2021).

[72] Poelstra (2015), Davenport (2019).

[73] This property of PoS has consequences for both fairness and security; see Cohen et al. (2021): p. 27.

[74] "Quadratic Proof of Stake" in Pillay (2020), for example, or "Robust Proof of Stake" as in Li et al. (2020).

[75] See Budish (2018): Section 3 for discussion.

[76] The question as phrased is about what is *good*. But in further research it may also be helpful to consider a parallel question about what is *right*.

REFERENCES

Aliapoulios, M., Ballard, C., Bhalerao, R., Lauinger, T., & McCoy, D. (2020). Swiped: Analyzing ground-truth data of a marketplace for stolen debit and credit cards. *Working paper*. https://krebsonsecurity.com/wp-content/uploads/2020/07/nyu-cardshop.pdf

Amnesty. (2018, October 29). Russia: New assault on independent media, NGOs and activists through suffocating fines. *Amnesty International*. https://www.amnesty.org/en/latest/news/2018/10/russia-new-assault-on-independent-media-ngos-and-activists-through-suffocating-fines/

Anderson, E. (2017). *Private government*. Princeton University Press.

Androulaki, E., & Karame, G. O. (2014). Hiding transaction amounts and balances in Bitcoin. In T. Holz & S. Ioannidis (Eds.), *Trust and trustworthy computing* (pp. 161–178). Springer.

Antonopoulos, A. M. (2015). *Mastering Bitcoin*. O'Reilly.

Auer, R. (2020). Beyond the doomsday ec onomics of "proof-of-work" in cryptocurrencies. *Globalization and monetary policy institute working paper no. 355*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3375168

Baradaran, M. (2015). *How the other half banks: Exclusion, exploitation, and the threat to democracy*. Harvard University Press.

Baradaran, M. (2017). *The color of money: Black banks and the racial wealth gap*. Harvard University Press.

Baradaran, M. (2020). Banking on Democracy. *Washington University Law Review*, *98*(2), 353–418.

Baraniuk, C. (2019, July 3). Bitcoin's energy consumption "equals that of Switzerland". *BBC News*. https://www.bbc.com/news/technology-48853230

Baydakova, A. (2020, July 15). Russian activists use Bitcoin, and the Kremlin doesn't like it. *Coindesk*. https://www.coindesk.com/russian-activists-use-crypto-kremlin-doesnt-like-it

Bendiksen, C., & Gibbons, S. (2019, December). The Bitcoin mining network. *CoinShares Research*. https://coinshares.com/assets/resources/Research/bitcoin-mining-network-december-2019.pdf

Benson, C. C., Jones, R., & Loftesness, S. (2017). *Payments systems in the US: A guide for the payments professional* (3rd Edition). Glenbrook Press.

Berg, C. (2018). Financial privacy. In *The classical liberal case for privacy in a world of surveillance and technological change* (pp. 181–194). Palgrave Macmillan.

Berg, C., Davidson, S., & Potts, J. (2020). Proof of work as a three-sided market. *Frontiers in Blockchain*, *3*(2), 1–5.

Biryukov, A., & Tikhomirov, S. (2019). Security and privacy of mobile wallet users in Bitcoin, Dash, Monero, and Zcash. *Pervasive and Mobile Computing*, *59*, 1–11.

Blanchette, J.-F. (2012). *Burdens of proof: Cryptographic culture and evidence law in the age of electronic documents*. MIT Press.

Bohannon, J. (2016). The Bitcoin busts. *Science Magazine*, *351*, 1144–1146.

Bonneau, J., Miller, A., Clark, J., Narayana, A., Kroll, J. A., & Felton, E. W. (2015). SoK: Research perspectives and challenges for Bitcoin and cryptocurrencies. *IEEE Symposium on Security and Privacy*, 104–121. https://doi.org/10.1109/SP.2015.14

Bridy, A. (2015). Internet payment blockades. *Florida Law Review*, *67*(5), 1523–1568.

Brito, J. (2019). The case for electronic cash: Why private peer-to-peer payments are essential to an open society. *Coin Center Report*.

Brooke, S., & Véliz, C. (2020, March). Views on privacy: A survey. *Data, Privacy, and the Individual*. https://docs.ie.edu/cgc/research/data-privacy/CGC-Data-Privacy-and-the-Individual-Report.pdf

Budish, E. (2018). The economic limits of Bitcoin and the blockchain. *NBER working paper no. 24717*. https://www.nber.org/system/files/working_papers/w24717/w24717.pdf

Carter, N. (2020, May 19). The last word on Bitcoin's energy consumption. *Coindesk*. https://www.coindesk.com/the-last-word-on-bitcoins-energy-consumption

Chowdhury, N. (2020). *Inside blockchain, Bitcoin and cryptocurrencies*. CRC Press.

Cohen, B., Hoffman, G., Edwards, M., & Stoops, C. (2021, February 9). Chia network business whitepaper. *Chia Business Whitepaper*. https://www.chia.net/assets/Chia-Business-Whitepaper-2021-02-09-v1.0.pdf

Cowen, N. (2020). Markets for rules: The promise and peril of blockchain distributed governance. *Journal of Entrepreneurship and Public Policy*, *9*(2), 213–226.

Dale, B. (2021, January 15). Lido protocol does Eth 2.0 staking but with a DeFi twist. *Coindesk*. https://www.coindesk.com/lido-protocol-does-eth-2-0-staking-but-with-a-defi-twist

Davenport, B. (2019, April 27). A stake to the heart. *Medium*. https://medium.com/@bendavenport/a-stake-to-the-heart-57fcd8ec323b

de Bruin, B., Herzog, L., O'Neill, M., & Sandberg, J. (2020). Philosophy of Money and finance. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy*. Winter 2020 Edition. https://plato.stanford.edu/archives/win2020/entries/money-finance/

DeCew, J. (2018). Privacy. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy*. Spring 2018 Edition. https://plato.stanford.edu/archives/spr2018/entries/privacy/

Dettling, L. J., Hsu, J. W., Jacobs, L., Moore, K. B., & Thompson, J. P. (2017, September 27). Recent trends in wealth-holding by race and ethnicity: Evidence from the survey of consumer finances. *FEDS Notes*. https://www.federalreserve.gov/econres/notes/feds-notes/recent-trends-in-wealth-holding-by-race-and-ethnicity-evidence-from-the-survey-of-consumer-finances-20170927.htm

Dierksmeier, C., & Seele, P. (2018). Cryptocurrencies and business ethics. *Journal of Business Ethics*, *152*, 1–14.

Fama, M., Fumagalli, A., & Lucarelli, S. (2019). Cryptocurrencies, monetary policy, and new forms of monetary sovereignty. *International Journal of Political Economy*, *48*, 174–194.

Flitter, E. (2020, June 18). "Banking while black": How cashing a check can be a minefield. *New York Times*. https://www.nytimes.com/2020/06/18/business/banks-black-customers-racism.html

Froomkin, A. M. (1996). The essential role of trusted third parties in electronic commerce. *Oregon Law Review*, *75*, 49.

Gervais, A., Karame, G. O., Čapkun, V., & Čapkun, S. (2014). Is Bitcoin a decentralized currency? *IEEE Security and Privacy*, *12*(3), 54–60.

Harper, C. (2019, May 8). Oil field alchemy: How Bitcoin can turn waste, emissions into proof-of-work. *Bitcoin Magazine*. https://bitcoinmagazine.com/articles/oil-field-alchemy-how-bitcoin-can-turn-waste-emissions-proof-work

Hasu, J. P., & Curtis, B. (2019, October). A model for Bitcoin's security and the declining block subsidy. *Uncommon Core*. https://uncommoncore.co/wp-content/uploads/2019/10/A-model-for-Bitcoins-security-and-the-declining-block-subsidy-v1.06.pdf

Hendrickson, J. R., Hogan, T. L., & Luther, W. J. (2016). The political economy of Bitcoin. *Economic Inquiry*, *54*(2), 925–939.

Hendrickson, J. R., & Luther, W. J. (2017). Banning Bitcoin. *Journal of Economic Behavior & Organization*, *141*, 188–195.

Herskind, L., Katsikouli, P., & Dragoni, N. (2020). Privacy and cryptocurrencies - a systematic literature review. *IEEE Access*, *8*, 54044–54059.

Hughes, E. (1993, March 9). A cyperpunk's manifesto. *Github*. https://github.com/NakamotoInstitute/nakamotoinstitute.org/blob/master/sni/static/docs/cypherpunk-manifesto.txt

Jackson, I. (2019). Bitcoin and black America.

Kahn, C. M., McAndrews, J., & Roberds, W. (2005). Money is privacy. *International Economic Review*, *46*(2), 377–399.

Kayyali, D., & Reitman, R. (2014, April 29). The morality police in your checking account: Chase bank shuts down accounts of adult entertainers. *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2014/04/moral-police-your-checking-account-chase-bank-shuts-down-accounts-adult

Kesari, A., Jay Hoofnagle, C., & McCoy, D. (2017). Deterring cybercrime: Focus on intermediaries. *Berkeley Technology Law Journal*, *32*, 3.

Kim, C., & Edgington, B. (2021, April 1). What Eth 2.0 meant in 2014 and what it means today. *Coindesk Podcast*. https://www.coindesk.com/podcasts/mapping-out-eth-2-0/eth2-0-staking-long-term-market-value

Kreimer, S. F. (2006). Censorship by proxy: The first amendment, internet intermediaries, and the problem of the weakest link. *University of Pennsylvania Law Review*, *155*(4), 11.

Kumar, R., & O'Brien, S. (2019, June 26). Findings from the diary of consumer payment choice. *FedNotes*, *Federal Reserve Bank of San Francisco*. https://www.frbsf.org/cash/publications/fed-notes/#2018

Kwecka, Z., Buchanan, W., Schafer, B., & Rauhofer, J. (2014). "I am Spartacus": Privacy enhancing technologies, collaborative obfuscation and privacy as a public good. *Artificial Intelligence and Law*, *22*(2), 113–139.

Lamport, L., Shostak, R., & Marshall, P. (1982). The byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, *4*(3), 382–401.

Lawson, B. (2013). Individual complicity in collective wrongdoing. *Ethical Theory & Moral Practice*, *16*(2), 227–243.

Li, A., Wei, X., & Zhou, He. (2020). Robust proof of stake: A new consensus protocol for sustainable blockchain systems. *Sustainability*, *12*(7), 25–69.

Li, F., & McMillin, B. (2014). A survey on zero-knowledge proofs. *Advances in Computers*, *94*, 25–69.

Luther, W. J. (2018, May). In defense of cash, 36–41. *Reason Magazine*.

Luther, W. J. (2020). Reglatory ambiguity in the market for Bitcoin. *The Review of Austrian Economics*, 1–14.

Luther, W. J., & Smith, S. S. (2020). Is Bitcoin a decentralized payment mechanism? *Journal of Institutional Economics*, *16*, 433–444.

Malcolm, J. (2017, March 15). Payment processors are still policing your sex life, and the latest victim is FetLife. *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2017/03/payment-processors-are-still-policing-your-sex-life

Mann, R. J., & Belzley, S. R. (2005). The promise of intermediary liability. *William and Mary Law Review*, *47*(1), 239.

Matsakis, L. (2019, July 20). How the West got China's social credit system wrong. *Wired*. https://www.wired.com/story/china-social-credit-score-system/

Matthews, S. (2010). Anonymity and the Social Self. *American Philosophical Quarterly*, *47*(4), 351–363.

Maurer, B., Nelms, T. C., & Swartz, L. (2013). "When perhaps the real problem is money itself!": The practical materiality of Bitcoin. *Social Semiotics*, *23*(2), 261–277.

McCook, H. (2014, July 19). Under the microscope: Conclusions on the costs of Bitcoin. *Coindesk*. https://www.coindesk.com/microscope-conclusions-costs-bitcoin

McDonell, S. (2019, June 7). China social media: WeChat and the surveillance state. *BBC News*. https://www.bbc.com/news/blogs-china-blog-48552907

McIntyre, A. (2019). Doctrine of double effect. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy*. Spring 2019 Edition. https://plato.stanford.edu/archives/spr2019/entries/double-effect/

Mitchell, B., & Franco, J. (2018). HOLC "Redlining" maps: The persistent structure of segregation and economic inequality. *NCRC*. https://ncrc.org/wp-content/uploads/dlm_uploads/2018/02/NCRC-Research-HOLC-10.pdf

Mooradian, N. (2009). The importance of privacy revisited. *Ethics and Information Technology*, *11*(3), 163–174.

Moore, A. D. (2018). Privacy, interests, and inalienable rights. *Moral Philosophy and Politics*, *5*(2), 327–355.

Nisbet, E. C., Stoycheff, E., & Pearce, K. E. (2012). Internet use and democratic demands: A multinational, multilevel model of internet use and citizen attitudes about democracy. *Journal of Communication*, *62*(2), 249–265.

Noble, S. U. (2018). *Algorithms of oppression: How search engines reinforce racism*. New York University Press.

Pease, M., Shostak, R., & Lamport, L. (1980). Reaching agreement in the presence of faults. *Journal of the ACM*, *27*(2), 228–234.

Pew. (2012). Payday lending in America: Who borrows, where they borrow, and why. *Pew charitable trusts*. https://www.pewtrusts.org/-/media/legacy/uploadedfiles/pcs_assets/2012/pewpaydaylendingreportpdf.pdf

Pickel, A. (1989). Never ask who should rule: Karl Popper and political theory. *Canadian Journal of Political Science*, *22*(1), 83–106.

Pillay, J. (2020, January). Quadratic proof of stake. *Ethereum Research*. https://ethresear.ch/t/quadratic-proof-of-stake-qpos/6842

Poelstra, A. (2015, March). On stake and consensus. *Lopp*. https://www.lopp.net/pdf/On-Stake-and-Consensus.pdf

Rachels, J. (1975). Why privacy is important. *Philosophy and Public Affairs*, *4*(4), 323–333.

Racsko, P. (2019). Blockchain and Democracy. *Society and Economy*, *41*, 353–369.

Rahn, R. (1999). *The end of money and the struggle for financial privacy*. The Discovery Institute.

Reid, F., & Harrigan, M. (2012). An analysis of anonymity in the Bitcoin system. In E. Altshuler & A. Cremers (Eds.), *Security and privacy in social networks* (pp. 197–223). Springer.

Reitman, R. (2012, Feburary 29). Legal censorship: PayPal makes a habit of deciding what users can read. *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2012/02/legal-censorship-paypal-makes-habit-deciding-what-users-can-read

Rettler, B. (2021, March 10). The rich get richer, the poor get Bitcoin. *Institute for Art and Ideas*. https://iai.tv/articles/the-rich-get-richer-the-poor-get-bitcoin-auid-1766

Rogoff, K. S. (2016). *The curse of cash*. Princeton University Press.

Rössler, B. (2005). *The value of privacy*. Polity Press.

Rothstein, R. (2018). *The color of law: A forgotten history of how our government segregated America*. Liveright.

Ruijgrok, K. (2017). From the web to the streets: Internet and protests under authoritarian regimes. *Democratization*, *24*(3), 498–520.

Stoycheff, E., & Nisbet, E. C. (2014). What's the bandwidth for democracy? Deconstructing Internet penetration and citizen attitudes about governance. *Political Communication*, *31*(4), 628–646.

Swire, P. P. (1999). Financial privacy and the theory of high-tech government surveillance. *Washington University Law Quarterly*, *77*, 461.

Tavani, H. T. (2007). Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy*, *38*(1), 1–22.

Tusikov, N. (2019). Defunding hate: PayPal's regulation of hate groups. *Surveillance and Society*, *17*(1/2), 46–53.

van den Hoven, J., Blaauw, M., Pieters, W., & Warnier, M. (2020). Privacy and information technology. In E. N. Zalta (Ed.), *The Stanford Encyclopedia of Philosophy*. Summer 2020 Edition. https://plato.stanford.edu/archives/sum2020/entries/it-privacy/

Véliz, C. (2019). The internet and privacy. In D. Edmonds (Ed.), *Ethics and the contemporary world* (pp. 149–159). Routledge.

Vincent, D. (2016, May 4). We looked inside a secret Chinese Bitcoin mine. *BBC Future*. https://www.bbc.com/future/article/20160504-we-looked-inside-a-secret-chinese-bitcoin-mine

Walch, A. (2018). Blockchain applications to international affairs: Reasons for skepticism. *Georgetown Journal of International Affairs*, *19*, 27–35.

Walch, A. (2019). Decentralization: Exploring the core claim of crypto systems. In C. Brummer (Ed.), *Cryptoassets: Legal, regulatory, and monetary perspectives* (pp. 39–68). Oxford University Press.
Warmke, C. (2021). Electronic coins. Manuscript. https://www.resistance.money/EC.pdf
Wigoder, N. (2019, May 9) Inside China's massive surveillance operation. *Wired*. https://www.wired.com/story/inside-chinas-massive-surveillance-operation/
World Bank. (2020). Remittance prices worldwide. *The World Bank*. https://remittanceprices.worldbank.org/en
Zuboff, S. (2019). *The age of surveillance capitalism: The fight for the future at the new frontier of power*. Profile Books.

AUTHOR BIOGRAPHIES

Andrew M. Bailey is an Associate Professor of Humanities/Philosophy at Yale-NUS College.

Bradley Rettler is an Assistant Professor of Philosophy at the University of Wyoming.

Craig Warmke is an Assistant Professor of Philosophy at Northern Illinois University.

How to cite this article: Bailey, A. M., Rettler, B., & Warmke, C. (2021). Philosophy, politics, and economics of cryptocurrency II: The moral landscape of monetary design. *Philosophy Compass*, e12784. https://doi.org/10.1111/phc3.12784