Cryptocurrency: Philosophy, Politics, and Economics[1]

Andrew M. Bailey, Bradley Rettler, & Craig Warmke[2]
Draft of 28 August 2020

Abstract

This article identifies a number of philosophically interesting questions about cryptocurrency. After describing what it *is*, how it *works*, and how it relates to orthodox conceptions of money, we map four dimensions across which cryptocurrencies vary, and some salient tradeoffs. A guiding theme in our discussion is that progress here requires a mixed approach that integrates purely technical results -- from, say, computer science and economics -- with philosophical insight.

1. Introduction

About a decade ago, the Bitcoin network was launched by its pseudonymous creator(s). It promised a revolution in how money works. Here at last, some thought, was an inclusive digital system for storing and transferring value that was inflation-proof, censorship-resistant, and independent of any oligarchic banking cartel.[3]

Bitcoin has spawned thousands of cryptocurrencies, and they command regular coverage in both popular media and research by computer scientists, economists, and lawyers. Their spectacular rise in valuation no doubt explains much of their popularity. Their use in scams and dark markets and the extravagant promises by blockchain proponents explain much of the rest.[4]

Yet there is more going on here than meets the eye. In the hopes of saying what that might be, this article identifies a number of philosophically interesting questions about cryptocurrency. Though we don't aim to answer these questions decisively, we do aim to show their significance and connection to important topics spanning philosophy, politics, and economics. We'll also introduce vocabulary required to approach these questions. Our goal is not to provide a *complete* primer, but rather to stimulate interest in the hopes that readers may eventually engage the issues themselves.

---

[1] We thank 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, and Roger Ver for helpful feedback or discussion.
[2] Order of authors is alphabetical.
[3] For readable histories of the ideological and technological innovations that led to Bitcoin, see Narayanan and Clark (2017) and Brunton (2019). Perhaps the most thorough study to date of the identity of its creator, "Satoshi Nakamoto", is in Frisby (2014): Chapter 6 and Appendix II.
[4] For extensive documentation that tells the story of the volatile reception of cryptocurrency, see Chowdhury (2020): Chapter 20.

We'll begin by characterizing what cryptocurrency *is*, how it *works*, and how it relates to orthodox conceptions of money. Then, we'll describe four dimensions across which cryptocurrencies vary and describe some tradeoffs involved in their having different combinations of features along those dimensions. A guiding theme in our discussion is that progress on these questions requires a mixed approach that integrates purely technical results -- from, say, computer science or economics -- with philosophical insight.

2. What cryptocurrency is -- and what it does

2.1 Cryptocurrency characterized

Cryptocurrencies are things like Bitcoin, Bitcoin Cash, Ethereum, Zcash, and Monero.[5] As we'll show, each of these behaves like *digital money*. But they're more than just digital money. Though money now often exists as a digital representation of value, it has little in common with Bitcoin or anything like it. For unlike traditional forms of digital money, cryptocurrencies deploy cryptography and novel network models to issue and transfer value. As we'll explain shortly, we take cryptocurrency to be digital money *that makes essential use of cryptography to manage and verify issuance and transfer of bearer instruments on a distributed ledger*.[6]

We'll often use Bitcoin as a focal case study. Here's why. First, it is the oldest and most well-understood cryptocurrency.[7] Bitcoin is thus the paradigm of paradigms, and much of what holds for it holds for other cryptocurrencies, too. Second, it is the most valuable and secure.[8] Third, and in part because of points one and two, Bitcoin enjoys significant network effects. The very fact that it is the most valued, studied, and well-understood cryptocurrency *makes* it an apt object of study. But since cryptocurrencies in general serve as our main target, we will often note how Bitcoin differs from alternatives.

[5] Better: cryptocurrencies are the native assets hosted by the Bitcoin, Bitcoin Cash, Ethereum, Zcash, and Monero networks -- (BTC, BCH, ETH, ZEC, and XMR, respectively) -- and things like them. The distinction here between a token and the network that sustains it is certainly relevant for a serious metaphysics of cryptocurrency. But we'll often elide it in the discussion to come.

[6] This is not far from the definition given in Ince (2013): "A digital payment system which employs cryptographic techniques to ensure security."

[7] It may be that there are networks *tied* with Bitcoin for longevity in virtue of sharing Bitcoin's first ("genesis") block; for detailed discussions of the metaphysics at play here, see Warmke (manuscripts a, b) and Carter et. al. (manuscript).

[8] At the time of writing, Bitcoin's total market capitalization was about six times larger than its closest competitor Ethereum's. On security -- roughly, how expensive it is to break the network's fundamental rules -- see Carter (2019).

2.2 How cryptocurrency works

We'll first describe how a specific cryptocurrency -- Bitcoin -- works, before elaborating on our definition. We'll keep things fairly simple; more technically-minded readers can follow the footnotes for more.[9]

We begin with the ledger. A ledger is a record of transactions. Your parents' checkbook has one. So does Bitcoin. But instead of documenting the movement of dollars across bank accounts, Bitcoin's ledger documents the movement of a digital commodity (amounts of Bitcoin) across various *addresses*. Whereas checkbook ledgers can go astray and differ from official bank records, Bitcoin's ledger -- known as its *blockchain* for reasons we'll discuss shortly -- cannot go astray, because for an address to have some Bitcoin *just is* for the ledger to say it does.[10]

Participants in the Bitcoin network fill three main, and non-exclusive, roles:

(1) *Users* broadcast transactions, i.e. send Bitcoin to each other.
(2) *Nodes* validate transactions and maintain copies of the ledger.
(3) *Miners c*ompete with one another to publish updates to the ledger.[11]

With the goal of uncovering some deeper questions, we'll spiral around these three roles until we gain a bird's eye view of the overall network. Once there, we'll also see how Bitcoin secures its ledger without relying on central authorities.

Nodes. Bitcoin's ledger isn't maintained by any particular person or bank but by thousands of computers running Bitcoin's ledger-keeping software.[12] Nodes serve as both *referees* and *curators*. As referees, nodes ensure that transactions follow certain rules before they can be added to the ledger -- for example, no address can spend more Bitcoin than it has.[13] Transactions that follow the rules are *valid*. When a miner attempts to add a batch of valid transactions to the ledger (see the next paragraph), the nodes check them once more. As curators, nodes also regularly update their individually stored copies of the ledger and share their copies of the ledger with other nodes, who in turn share theirs with other nodes -- and so on. Updates to the ledger propagate quickly across the entire network.

---

[9] The most accurate yet accessible resources for understanding Bitcoin include Antonopoulos (2015) and Rosenbaum (2019). Another useful and practically-minded approach, intended for a developer audience is Song (2019). Lopp (2020) is the most responsible, up-to-date, and compendious collection of online resources for understanding Bitcoin, usefully categorized and ranging from elementary to advanced.
[10] Glazier (manuscript).
[11] A fourth category of participant includes those who maintain Bitcoin's software. For details about one group of Bitcoin software developers, see Lopp (2018).
[12] Anyone with internet access can download the software and operate a node. What we're calling a "node" is, more precisely, a *full* node. There are presently about 10,000 active full nodes, and 90,000 more running outdated versions of the software.
[13] For a complete list of the relevant rules, see https://en.bitcoin.it/wiki/Protocol_rules#Transactions.

Miners. Updates to the ledger come around every ten minutes. That's when a miner has won a competition to publish the next *block* of transactions, which are then added to the block*chain* (which is Bitcoin's ledger). A winner in this recurring competition solves a computationally difficult math problem by trial and error before anyone else.[14] To solve such a problem, each miner feeds a cryptographic algorithm information about the next batch of transactions along with a random number. The algorithm garbles the inputs unpredictably into a single number, and the competitors hope that as they cycle through different random numbers, the algorithm eventually spits out a numerical value that starts with at least a certain number of zeroes. Whoever finds such a value first wins the right to update the ledger with a new block, one that includes a transaction that mints an amount of Bitcoin for the winner's address.[15] All Bitcoin that will ever exist has come or will come from such rewards. When the network first began, miners won 50 Bitcoin per block. Every four years, the reward halves. Nowadays, a miner wins 6.25 Bitcoin each block.

When a miner wins, it propagates its block to nodes, who will add it to their copies of the ledger if they judge that it follows the rules, and then share that newly updated ledger with other nodes. The ledger thereby grows block-by-block. Each block bears a cryptographic mark of the previous block, namely the solution to the previous block's cryptographic problem. These marks order the ledger's blocks into a chain --- a *blockchain*.

Sometimes, multiple miners produce winning blocks at around the same time. Here, the chain splits, and some miners may begin to build on different sides of the chain. How does the network decide which version of the ledger to endorse without relying on a central authority? Nodes follow a rule to endorse the chain with the most accumulated *proof of work*, the chain whose blocks likely took the most processing power to create. This is how the network achieves consensus without central authorities.

Instead of digging into earth's crust for precious metals, Bitcoin miners marshal computing power to "dig" into the mathematical realm for a lucky number that will net them new Bitcoin. Bitcoin mining is no less subject to the quest for increased power and efficiency. But the issuance schedule doesn't speed up when miners marshal increasing amounts of energy; rather, the network adjusts the prize difficulty to ensure that some miner continues to win around every ten minutes.[16]

---

[14] This way of deciding who gets to add to the blockchain takes a lot of computing power, and so is called a *proof of work*. See "Consensus" section for more.

[15] In 2140, a final new amount will be created, and from then on the only way to get more will be to receive from an address that already has some. People that keep the ledger updated will no longer win new amounts for doing so, but will instead win amounts entirely from transaction fees.

[16] Every 2016th block, nodes adjust the difficulty as required: if, during this time, it took on average less than ten minutes to win, the problems get harder; but if it took on average more than ten minutes to win, they get easier.

Users. So, miners compete to publish blocks of transactions, and nodes verify and store them as a growing blockchain. But where do the transactions come from in the first place? With the help of a free software application, anyone can write a transaction that the nodes will judge as valid. In the simplest case, a valid transaction includes four pieces of information. The first two require no explanation:

(i) an amount of Bitcoin to send
(ii) a recipient address

But the next two pieces require a little more. Together, (i) and (ii) form a transaction's *output,* and each output has a unique identifier in the blockchain. Your *new* transaction must also identify a *previous* transaction output in which *your* address was the recipient by including its identifier:

(iii) the identifier for an output to your address

Your transaction will also need to show proof that you own the Bitcoin in that previous output. This proof comes by way of a *digital signature*. Where does the digital signature come from and how does it provide proof of ownership? Every address has a unique password or *private key*. (Indeed, the private key itself generates its paired address through a cryptographic function.[17]) To provide your digital signature, you (privately) feed the address's private key along with the rest of the candidate transaction (the info from (i) through (iii)) into a special cryptographic algorithm. The signature then comes out the other end. So, in addition to (i) through (iii), your transaction needs:

(iv) a digital signature from the private key for the address that received Bitcoin in (iii)

No one sees the private key, but due to the aforementioned relation between it and its address, anyone can verify whether the appropriate private key helped produce the digital signature. And nodes do exactly that. Your software application strings (i) through (iv) together into a transaction and sends it to nodes for validation.

Now let's put the pieces together. Suppose you want to send some Bitcoin to Dorian. You specify an amount to send, an address Dorian controls, and a previous transaction output, yet to be spent, in which *your* address received some Bitcoin. Then, your application sends the transaction along with the appropriate digital signature to the nodes.[18] The nodes verify the signature and check the ledger to make sure that you're not trying to spend Bitcoin that's already been spent or trying to spend more Bitcoin than you have. The nodes that validate the

[17] The function is some kind of elliptic curve cryptography; Bitcoin uses secp256k1. For an accessible, non-book-length explanation, see Warmke (manuscript b).
[18] Bitcoin wallets such as Bither or Electrum make this user-friendly. Initiating a transaction is very much like -- and about as easy as -- sending an email.

transaction then forward it to the miners, who race to publish it in the next block.[19] The winning miner sends its block with the solution for the nodes to verify. Once verified, the nodes add the block. This is how the chain grows: block by block (645,259 times, so far).

Despite Bitcoin's permissionless architecture, it remains secure and the cryptographic derivation of addresses from private keys protects users. First, derivation is one-way; it is practically impossible -- even for the NSA or Google -- to seize Bitcoin by searching for an address's private key. Second, transacting Bitcoin doesn't require registration with a central authority. Since private keys are mathematical objects, a user can simply use a computer to pluck one from the mathematical realm. And, third, since the relation between private keys and addresses is purely mathematical, this information needn't be stored on centralized and vulnerable servers.

And yet the most innovative aspects of Bitcoin's security aren't purely cryptographic or mathematical. When a ledger like Bitcoin's dictates who has which amounts of a valuable commodity, some will inevitably try to alter the ledger in self-serving ways. Bitcoin's ledger strongly resists this kind of attack by incentivizing honest behavior and making cheating costly. It does this by luring participants into competing for scarce rewards in a way that protects both the network's integrity and the scarcity of the rewards themselves.

This requires some unpacking. Calvin wishes to tamper with the ledger for fun or profit. How might he proceed?

He could add a transaction to a block -- sending Bitcoin to himself without a signature from an originating address, or from an address without sufficient funds, for example. But such blocks would be invalid and rejected by other nodes for breaking protocol rules. What Calvin needs is a way to cheat the system that isn't transparently invalid. Here's one: Calvin could try to *double-spend* by spending Bitcoin to an address (for dollars, say) before rolling back the chain to send the very same Bitcoin to a *different* address. He'd do this by attempting to replace the block that contained his transaction with a new block containing a transaction that sent his Bitcoin elsewhere. Then he'd hope that other nodes accept his new block as part of the official chain.

But remember: each block bears a cryptographic mark of the previous block's transactions and provides a tamper-resistant ordering of all blocks. Subsequent blocks verified by *other* nodes wouldn't bear the mark of Calvin' new block. Calvin will, then, have forged a new and diverging branch of the blockchain. Nodes wouldn't follow that branch unless it represented the most accumulated proof of work. And it wouldn't, since Calvin's chain wouldn't show all the work that had been done since the block that contained his transaction.

Calvin could conceivably marshal enough computing power to ensure that his branch of the blockchain attains the most accumulated proof of work. This is called a *51% attack* because an

[19] Users can also incentivize miners to include their transactions by offering a fee to the winner.

attacker with 51% of the network's total computing power is virtually certain to build the strongest branch. With enough power, Calvin can effectively roll the ledger back and add enough blocks, one-by-one, until the nodes recognize his chain as the strongest.[20] But the attack is unlikely to succeed, since Calvin would have to produce many winning blocks in a row -- an enormously expensive task in terms of both hardware and energy, and by no means guaranteed to succeed.[21] What's worse, even if Calvin succeeds, the cheating itself may undermine the operation's entire purpose. People could look to the publicly available blockchain and see what happened. Consequently, many would trust Bitcoin less, sell it, and sink the value of Calvin's spoils below the cost of its plunder, or at least below the value of the rewards Calvin could have attained honestly. The rest of the network could also coordinate to reject Calvin's blocks, sending the value of Calvin's rewards to zero. With Bitcoin, cheating just doesn't pay.

A network with incentives like those described in this section enjoys security on a variety of fronts. Provided that its native token has some value, it's not hard to see how it could function as a distinctive kind of payment system -- a new way to store and transfer value without banks or other legacy financial institutions.[22]

---

[20] For metaphysicians, think of this like changing "the past" in a growing block universe, where the leading edge reverses back, allowing one to add time-slices that differ from the ones having previously occurred.

[21] We explain why in Section 6.

[22] This article focuses on *monetary* uses of cryptographically secured distributed ledgers or blockchains: on crypto*currency*. But these do not begin to exhaust the alleged uses of blockchains. Theoretically, any application that involves storing entries in a ledger *could* operate on a blockchain; see Bonneau, et. al (2015), 1. This thought has inspired a number of extraordinary claims about the power of "blockchain technology" to revolutionize or transform. Alleged use cases for blockchains include elections and voting, corporate governance, prediction markets, supply chain management, file storage, legal identities, foreign aid, video game collectibles, medical records, and more. The list sounds impressive!

But some caveats support a cautious approach. First, blockchains in service of cryptocurrency are by now a widely-used and reasonably well-understood phenomenon. They have an empirical track record of *working*; Bitcoin has remained in operation for about a decade, for example. The same cannot be said for any other use. Second, it is clear how monetary uses of a blockchain contribute to the ongoing sustenance of a host blockchain: those who maintain the network (miners, say) receive value in the form of digital tokens (Bitcoin, say) for doing so. It is much less clear what incentives are supposed to contribute to the sustenance and security of a blockchain without such tokens at stake. We're not so optimistic that incentives of the right kind (to cultivate a blockchain and abide by its constitutive rules, that is) could be maintained without such a token -- without a native cryptocurrency to serve as a reward, that is. Third, and relatedly, we think of cryptocurrency as providing the *base layer* upon which other applications can be built. Our aim has been to understand that layer, with the conviction that this understanding is a prerequisite for responsible analysis of applications that build on that layer. Fourth, proponents of blockchain technology beyond cryptocurrency applications have, in almost every instance we know of, failed to make a case that a distributed ledger is in fact appropriate for the use case in mind. In most non-currency cases, a traditional centralized database is far more efficient than any distributed alternative, since one doesn't need to prevent double-spending attacks.

2.3 Cryptocurrency characterized again

We are now in a position to better explain our characterisation of cryptocurrency as *digital money that makes essential use of cryptography to manage and verify issuance and transfer of bearer instruments on a distributed ledger*. Let's take each piece in turn.

> Digital: cryptocurrencies are inherently digital and need not involve any concrete material representation of value (in contrast to, for example, paper bills issued by a state).
>
> Money: cryptocurrencies, to some extent, enjoy some classical properties of money, like divisibility, portability, and fungibility. Whether they are apt stores of value, means of exchange, or units of account is more contentious, and something we'll take up below.
>
> Essential use of cryptography: cryptocurrencies do not just use cryptography. They do so essentially. Only cryptographic algorithms provide the verifiable but one-way garbling necessary for doing things like generating addresses from passwords, minting and transferring tokens, and providing a tamper-resistant ordering of blocks.
>
> Bearer instruments: in contrast to registered securities (where ownership is centrally logged and recoverable should concrete proof of ownership go missing), ownership and transfer of a bearer instrument requires no settlement beyond possession. Cryptocurrencies, in this respect, resemble bearer instruments. But possession of a token, in this case, typically *just is* control of its associated private key (its "password"). To lose the password is to lose the asset.
>
> Distributed ledger: record-keeping of the issuance and transfer of *traditional* digital currencies is typically centralized, taking place in, for example, a database to which only trusted banks have access. Issuance and transfer of *crypto*currency tokens, by contrast, typically occur across a network and often, but not always, through a blockchain, a special kind of append-only record.[23]

[23] Chowdhury (2020): 24 offers a useful taxonomy of distributed ledgers and their key technical and social properties.

3. Is cryptocurrency money? Should it be?

3.1 Three questions about money

We've said cryptocurrencies have, to some extent, money-like properties -- we've called them "digital money". *Are* they money? Many proponents *aspire* for cryptocurrencies to be *used* as money, but are these aspirations realistic? Three points will guide further discussion.

First, *money* is a functional kind.[24] For something to be money is not for it to consist of some special material or have a particular origin story.[25] Rather, something -- whether paper notes, digital representations of value, cigarettes, or gold bars -- is money to the extent that it fills a cluster of roles.[26] Standard candidates for those roles include being a unit of account, store of value, and means of exchange.[27] We can refine our question, then: to what extent does cryptocurrency fill these money roles?

Second, many cryptocurrencies exemplify distinct technical, economic, and political features.[28] It will not be very useful to inquire, then, whether cryptocurrencies *in general* fill key money roles. That's like asking whether rocks are doorstops. We would do better to ask, of a particular cryptocurrency X, whether *it* fills these key money roles.

Third, our refined question comes in various flavors:

a) Modal: to what extent *could* X fill key money roles?
b) Actual: to what extent does X, *in fact*, fill key money roles?[29]

---

[24] For philosophical treatment of the ontology of money that connects its functional role with a number of normative issues, see Zelmanovitz (2016).
[25] Compare *being a weapon* or *being a musical instrument*. What sorts of things can be musical instruments? Weapons? Very many -- as long as they *do* what a musical instrument or weapon does. So also with money.
[26] One way to elaborate on money as a functional kind goes like this. Write out all the things money *does* and the roles it *plays* in economic theory. Add to that the claim that something in fact *does* and *plays* accordingly. The resulting sentence -- the "Ramsey sentence" for money -- tells us much about what money is. We can learn even more through empirical inquiry into what in fact satisfies that Ramsey sentence. For more on this approach to defining theoretical terms, see Lewis (1970).
[27] The list given here is a mainstay in economics textbooks with some slight variations (1875). Jevons (see Chapter 5), following Chevalier (1854) and Harris (1757), also identifies some "material qualities". Some claim that nonmonetary value (what economists call "intrinsic value") is required; for a discussion of this applied to Bitcoin, see Luther (2018c). DuPont (2019: Chapter 3) argues that orthodox views about money and its functions -- as adopted and promulgated by cryptocurrency proponents, at least -- are more an evangelistic and self-fulfilling myth than anything else. For a theoretical treatment of the improvements to efficiency that money as a medium of exchange enables, see Kiyotaki and Wright (1989).
[28] Thousands, in fact. For a list, ordered by market capitalization, see https://coincap.io/
[29] Smit et. al. (2016) sharpens the Modal and Actual questions.

c) Normative: Supposing that X *could* fill key money roles, would it be all things considered *good* for it to do so?[30]

The first question is largely technical. It turns on the degree to which X is, or could be, portable and divisible and so on.[31] The second is partly empirical and turns on the actual *uses* of X.[32] The third is all that and more, and much of what we'll say addresses it in some way or other.

To see the import of normative inquiry here and its distinction from more technical and empirical questions, consider an analogy to another functional kind. We could ask of a given thing whether it could be a musical instrument, or whether it is being presently used as a musical instrument. We'd then examine its shape, mass, acoustic profile, and so on. Whether it is or could be a musical instrument isn't that interesting. But the question about whether it *should* be used as a musical instrument -- whether it would be *good* for it to be so used -- will implicate a host of other factors. Is it alive? Expensive? Environmentally damaging? Malodorous? These questions take us beyond physics and geometry.

So also with cryptocurrency as money. There are purely technical and empirical questions about what cryptocurrencies are or could be.[33] But deeper and more complicated questions lurk nearby that go well beyond the technical and empirical: *should* cryptocurrencies fill key money roles?[34] What are the costs and benefits of cryptocurrencies' filling those roles instead of state-issued fiat currencies, precious metals, or something else besides? To whom do those costs and benefits accrue?

---

[30] So Sidgwick (1879): "Let me then raise once more the vexed question - What is money? But first, we must observe that when proposed in this form the problem is fundamentally ambiguous; as it blends the two quite distinct questions, (1) What do we call money? and (2) What *ought* we call money?"

[31] For a fascinating treatment of how a currency's denomination affects its eligibility for the medium of exchange function, see Albrecht, Hawkins, and Duffin (2020).

[32] The first two questions have received ample treatment in the literature. Ammous (2018a) offers a helpful and empirically informed treatment of the modal and actual questions. Other helpful treatment of these questions -- both of which answer mostly in the negative can be found in Kubát (2015) and Yermack (2015). Hazlett and Luther (2019) reply to Yermack. Baur et. al. (2018) argue that a minority of users treat Bitcoin as a medium of exchange and that most treat it as a speculative asset; but they fail to note that these uses are compatible. Explicit discussion of the Normative question is scarce; the present article fills that lacuna.

[33] These questions have future-tensed counterparts too; see England and Fratrik (2018) and Luther (2016b). For discussion of three related factors that tell against cryptocurrencies currently being money -- high transaction fees, long transaction times, and volatility in valuation against fiat currencies -- see Fama et. al. (2019): 177. For a theoretical but very useful treatment of the role of volatility in a currency's utility as a means of exchange, see Schilling and Uhlig (2019).

[34] We disagree, then, with the hypothesis that Bitcoin or other cryptocurrencies are neutral or "neither good nor bad", as in Brito and Castillo (2013): 34.

3.2 Varieties of cryptocurrency

Thus far, we've given a primer on what cryptocurrency is, how it works, and its status as money. The technical difference among cryptocurrencies lead to normative differences. We organize the rest of our discussion around four:[35]

> Privacy: can *everyone* see the sending address, the receiving address, and the amount of any transaction? Some privacy-focused cryptocurrencies allow for shielded or private transactions where the sending address, 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, and who, if anyone, gives permission to do so? Are there centralized chokepoints whereby some entities can censor transactions?
>
> Consensus: how does a network agree on new entries to the ledger or issue new amounts? Some cryptocurrencies do not involve solving math problems in order to create new amounts or add entries to the ledger. They might, instead, simply require proof of having the password to some amount.
>
> Monetary Policy: is there a hard limit to the creation of new amounts? Some cryptocurrencies, in contrast to Bitcoin, impose no eventual limit on the creation of new amounts. Some instead deploy a fixed number of tokens created at that currency's genesis. Some have both "pre-mined" tokens and the creation of new tokens.

These blend technical, economic, and normative matters. For example, on the first dimension: is financial privacy good? For whom? Against what does it trade off, and what are the costs and benefits of implementing transactions that cannot easily be tracked or monitored? On the second: should people need *permission* before being able to use a financial system? From whom? On the third: who should be in charge of a ledger? Is the use of vast computational resources to cultivate a network worth it? What are the costs and benefits of such a system and how do they stack up against possible alternative models? And on the fourth: what are the consequences, costs, and benefits of an inflationary issuance schedule? Who stands to lose or gain?

In what remains, we explore these questions in more detail and assess answers to them.

[35] For a dated but nonetheless helpful and systematic treatment of a number of cryptocurrencies and their features (with an eye towards those that can be decoupled), see Bonneau et. al. (2015).

4. Privacy

4.1 Financial privacy under threat

Someone enjoys privacy to the extent that others have limited access to her personal information and personal space.[36] For our purposes, we need not precisely settle just what kinds of information or space count as "personal". And we'll focus on information privacy. What matters for our purposes is the plausible hypothesis that *financial* information -- information about wealth, income, buying, selling, and so on -- qualifies as personal.[37]

Privacy has seemed to many a *pro tanto* good; it makes us better off in some respects.[38] Privacy is seemingly a final good; but it also evinces instrumental value in enabling social relationships, contributing to human dignity, and facilitating variety in lifestyle.[39] 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.[40] Despite widespread agreement on the value of privacy, however, *financial* privacy -- privacy with respect to buying, selling, and storing value -- is not so widely discussed or defended. As we'll see, though, it deserves renewed attention. And though financial privacy continues to erode, cryptocurrencies provide new tools for protecting it.

A variety of factors contribute to declining financial privacy: a rise in corporate and state surveillance capacity, use of credit in everyday consumer transactions (and the decline in the use of physical currency in everyday consumer transactions), big data, and so on.[41] More eyes vie for personal financial information with fewer checks on the power to acquire it.[42] Something valuable seems under systematic threat. Private corporations now collect, analyze, trade, and act

[36] This definition loosely follows that in Véliz (2019), 149. Tavani (2007) defends a more capacious and mixed account of what privacy is including elements of both *access* and *control*. Rössler (2005: 9ff) offers a helpful discussion of the kinds of privacy beyond those included in our definition. For an overview of philosophical work on privacy, see DeCew (2018) and, with a special eye towards privacy and information technology, van den Hoven et. al. (2020).

[37] You may test the hypothesis for plausibility by monitoring your own reactions to the fact that every purchase you've ever made is now a matter of public record. For convincing arguments that financial privacy is indeed a form of privacy with some value, see Berg (2018).

[38] That there are constitutional protections for privacy across over 20 countries is strong evidence of this claim, we think. See also Brooke and Véliz (2020) for straightforward survey evidence: "1,107 people responded to the survey… 82% deemed privacy extremely or very important, and only 1% deemed privacy unimportant."

[39] A classic statement of the idea that privacy makes social relationships possible -- as when one reveals personal information to one's doctor but not to one's friends -- is Rachels (1975). Mooradian (2009) connects Rachels' account of the importance of privacy to recent developments in the digital age.

[40] On whether privacy is an inalienable right or merely an unimportant interest (and the spectrum of options between these extremes), see Moore (2018).

[41] See, e.g., Kumar and O'Brien (2019).

[42] See Rahn (1999) for a chilling and prescient expression of this trend -- in particular, the role of digital money in declining financial privacy.

on huge swaths of personal financial data, resulting in a kind of "surveillance capitalism" that should concern those indifferent to state-led encroachments.[43]

We face, then, an uneasy dilemma between convenience and privacy. We could stick to the convenience of credit cards and bank accounts and give up on financial privacy.[44] Or we could renounce credit cards, bank accounts, PayPal, and other easily traceable payment tools in favor of physical currency. Doing so would certainly secure some measure of financial privacy. But we would incur enormous costs of convenience by forgoing quicker and simpler payment tools, access to credit, and other financial instruments.

4.2 Solutions

Can cryptocurrencies resolve the dilemma? In its current form and as typically used, Bitcoin does not provide users with significant financial privacy.[45] The Bitcoin ledger is public. And its record includes all amounts, destinations, and sources. These destinations take the form of random-seeming strings of characters (addresses) that give a veneer of pseudonymity. The Bitcoin ledger itself does not associate addresses with real-world identities like legal names, phone numbers, birth dates, and so on. But such associations are not difficult for state and corporate entities to establish, especially since regulated exchanges require customers to provide identifying information.[46]

Other cryptocurrencies (or supplementations to Bitcoin, as usually used) differ crucially in this respect.[47] They provide users with two methods for resisting surveillance: *shielding* and *obscurity*.[48] 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. But shielded transactions still provably abide by the network rules. Perhaps the most well-known shielding strategy that enables this surprising combination of secrecy and provable validity involves *zero-knowledge proofs*.[49] In a system with zero-knowledge proofs, like Zcash,

[43] We borrow the evocative and useful phrase "surveillance capitalism" from Zuboff (2019) as it highlights that states aren't the only adversaries to worry about here.
[44] For an expression of a dilemma along these lines that predates the emergence of Bitcoin and other cryptocurrencies, see Kahn et. al. (2005).
[45] One fascinating early treatment of anonymity and privacy within Bitcoin in particular is Reid and Harrigan (2012). Bohannon (2016) is a vivid account of the degree to which Bitcoin, as standardly used, is neither anonymous nor private.
[46] For details on some of the tools used by corporations and state authorities -- sometimes called *blockchain analysis* -- see Herskind et. al. (2020): 54049.
[47] There's some irony in new privacy tools emerging from digital money since the digitalization of finance has been an important *threat* to privacy. For more, see Blanchette (2012: 6).
[48] The distinction we draw here is similar to that Herskind et. al. (2020) draw between hindrances to graph analyses of ledger activity that are "Zero-knowledge based" or "Decoy-based".
[49] For a useful overview of zero-knowledge proofs and their applications, see Li and McMillin (2014). Androulaki and Karame (2014) offers a dated but helpful discussion of Bitcoin's native privacy limitations and extending Bitcoin with zero-knowledge proofs.

users can send and receive value on a public ledger without revealing any information about amounts, destinations, and sources.[50]

By *obscurity*, we mean privacy gained through anonymity within a group.[51] Obscured transactions drive a wedge between the real-life identities of users and financial details fully visible on a ledger. One obscuring strategy -- implemented by Monero -- deploys *ring signatures*. Each transaction involves a ring of possible sources (instead of, say, one originating address and one associated private key, as one might find in some Bitcoin transactions). Only the originating user knows which member of the ring is the true source; outside observers and receiving parties simply cannot tell.

Another obscuring method involves multiple users sending value back to themselves at new addresses in a single transaction. In such a "CoinJoin" transaction, users sever their identities from the tokens held at their old addresses. Since, in Bitcoin, a 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. 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.[52] So even if we had known who had which Bitcoin at which addresses going in, we wouldn't know who or how many received how much Bitcoin on the other end.[53]

The main point here is that cryptocurrencies promise their users a financial Ring of Gyges that breaks the dilemma outlined above. We need not sacrifice privacy for convenience. To a large extent, we can have both, by using, for example, Bitcoin (with CoinJoin), Zcash, or Monero. The promise isn't merely hypothetical, since cryptocurrency networks currently process millions of transactions per hour. Nor must we wait on public policy, since individuals can already use a privacy-enhancing cryptocurrency at any time. Indeed, cryptocurrencies offer tools to protect privacy interests even in the face of corporate or state power (see "Censorship-Resistance", below, for more).

Financial privacy achieved through either shielding or obscurity has a network effect. The more transactions are protected in this way, the stronger that protection becomes.[54] This holds

---

[50] The Zcash protocol as presently implemented does require a *trusted setup* and may be vulnerable to privacy attacks from state-level adversaries that target, e.g., transaction timing or network activity. For more detailed discussion and citations, see Herskind et. al. (2020).

[51] For a careful philosophical treatment of the relationship between anonymity and privacy and the value of the former, see Matthews (2010).

[52] Here's what a CoinJoin transaction looks like on the blockchain: https://www.blockchain.com/btc/tx/e4abb15310348edc606e597effc81697bfce4b6de7598347f17c2befd4febf3b

[53] For more, see Biryukov and Tikhomirov (2019): 10.

[54] On privacy through obscurity as a *public* good -- non-rivalrous and non-excludable -- see Kwecka et. al. (2014).

especially for privacy through obscurity.[55] It is precisely the presence of a swarm of indistinguishable transactions (or participants in a ring signature) that makes those transactions private. The bigger the swarm, the better the privacy. There are, accordingly, ethical consequences to joining such a swarm. Users who participate, whether as miners or transactors, are not just securing privacy for themselves -- they're securing it for others as well, including those with potentially nefarious purposes. There are obvious upsides to this -- positive externalities, economists would say. But there are downsides too -- negative externalities.[56] For privacy can be used for both good or ill. *Double-effect* reasoning may be useful here, according to which, roughly, subjects are not morally responsible for the foreseeable consequences (in this case, securing privacy for bad actors) of an action provided that those consequences are not intended.[57]

We'll close with a quick argument. Cryptocurrencies provide viable tools for promoting financial privacy. Cryptocurrencies exemplify, then, an important instrumental value. The argument doesn't end there, of course. A full evaluation would require weighing the goods promoted here against those that are thwarted.[58] But the argument does illuminate one path towards an affirmative answer to our normative question about cryptocurrency and money: *yes, it is good to use cryptocurrency as money, because doing so promotes privacy*.

One can affirm a view along these lines without taking privacy to be a *final* good. Privacy may, instead, be good only because it is instrumental in promoting other goods. We'll below identify the role of privacy in promoting permissionlessness and thus in resisting state and corporate censorship. Another good promoted by the kind of privacy in view is *fungibility*. When third parties simply can't tell whether a given transaction has "tainted ancestors" (is derived from transactions that are themselves of dubious moral or legal provenance), they have strong reason to be indifferent between, say, amounts of Bitcoin from different sources. Fungibility, as we've observed above, contributes to capacity for playing key money roles. It's interesting, then, that the very kinds of privacy that could make cryptocurrencies distinctive from traditional money could also make them better suited for traditional money roles.

---

[55] The point applies to privacy through shielding too, since shielded transactions may be subject to timing or network traffic analysis even when the amount, source, and destination are as of yet unknown. The more transactions there are at a given time or through a given network path, the less useful this analysis becomes -- the certainty with which it can deliver unmasking verdicts drops dramatically.

[56] One worry, then, is that in contributing to the privacy of transactions in general, one is *complicit* in the harm wrought by nefarious transactions. On complicity, see Lawson (2013).

[57] See Dierksmeier and Seele (2018) for related points. On double-effect reasoning in general, see McIntyre (2019).

[58] For a forceful presentation of the objection that financial privacy is not an unqualified good, since it facilitates all manner of insalubrious activity, presented as an argument against physical currency and the anonymous or private transactions it enables, see Rogoff (2016), especially Chapter 5. Luther (2018a) replies to Rogoff. For robust replies to a number of general concerns about the harms of privacy, see Swire (1999).

5. Censorship-resistance

We've noted that the ubiquity of cashless transactions erodes financial privacy. But many of those who sit atop financial superhighways and *track* our purchases also have the power to *prevent* them. Cryptocurrencies can also protect against state or 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.[59] We'll first describe how state and corporate entities presently control who has access to financial systems.

5.1 Permissioned payments

We increasingly transact by sending digitized information through multiple parties on a payment network.[60] More visible parties provide consumers gateways to the network with cards and software applications to initiate transactions. Less visible parties -- e.g. intermediary banks and clearinghouses -- authorize, clear, and settle those transactions.[61]

We'll call a party on a payment network an *authority* when it can reliably block transactions on the network.[62] Blocking can take a number of forms. Entry points like Venmo may deny you access and prevent you from initiating a transaction on their platform. Intermediaries like Wells Fargo may deny you service or, short of total denial, block transactions of certain kinds, or even particular transactions. While authorities like these might block transactions from taking a particular path through a network, they can't stop transactions from taking a detour through other authorities. But an unavoidable hub in a payment network, e.g. a central bank, can block someone from using the 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, whether that's a political affiliation, religious commitment, career, or level of credit. In entity-centered blocking, authorities might block transactions from a particular organization, like a non-profit watchdog, or a particular person, like the outspoken whistleblower. But instead of blocking all transactions from particular people or organizations, an authority might block

---

[59] Many here contrast *centralized* and *decentralized* payment networks, with Bitcoin and other cryptocurrencies as alleged 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; on this point see Walch (2018) and Walch (2019). Second, Luther and Smith (2020): 437 offer a convincing argument that the better term here for networks like Bitcoin is *distributed*, since they rely on an entire network to clear payments.

[60] Raynil and O'Brien (2019).

[61] On payments systems in the US, see Benson et. al. (2017).

[62] Authorities, as we conceive of them, are a kind of trusted third party, since they stand *between* the more obvious parties to a given transaction. See Froomkin (1996).

certain kinds of transactions, like transactions involving drugs, pornography, or copyright infringement.[63]

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. So let's say that a payment network is *permissioned* when it has one or more authorities.

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

5.2 Financial censorship illustrated

This has been a bit abstract; we may benefit from reviewing some cases of financial censorship:

> Marijuana. Some states in the US 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.[64]
>
> 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.[65] In 2014, JPMorgan Chase terminated the accounts of many involved in the adult film industry.[66] This came on the heels of Chase refusing to process payments for Lovability, an online condom store.[67] And, in 2017, the adult social network FetLife saw its payment services revoked.[68]
>
> Remittances. Cross-border payments often involve migrants sending money home in payments routed through fee-extracting authorities. Globally, the average remittance fee

[63] Bridy (2015).
[64] Baradaran (forthcoming).
[65] Reitman (2012).
[66] Kayyali and Reitman (2014).
[67] Kayyali and Reitman (2014).
[68] Malcolm (2017).

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%.[69] 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 -- donations funneled through a conventional bank account, for example -- are closed off or made costly through fines, legal harassment, frozen bank accounts, and so on.[70]
>
> 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.[71] 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.[72]

5.3 Financial censorship is dangerous

Many readers will be troubled by at least some of these cases. Still, some may resist the overall point here on the grounds that (apparent) abuses of authority are to be balanced against some good they enable, such as preventing transactions involved in illegal drugs, money laundering, terrorism, copyright infringement, and, more globally, efforts to avoid economic sanctions. We're not so sanguine for a familiar and potent reason. The power to block illegal transactions is also the power to block legal transactions. And although some may cheer at the financial censorship of unpopular but law-abiding entities, the revolving door of authorities suggests that it won't be long before the shoe is on the other foot.[73]

---

[69] Data from World Bank (2020).
[70] Amnesty (2020).
[71] See Wigoder (2019) and McDonell (2019), for example.
[72] Matsakis (2019).
[73] So Brito (2019), 20-21: "Today it may be gun advocates that are targeted, but tomorrow it could be abortion providers that are dropped by financial intermediaries. Groups such as Muslim charities, sexual fetishist communities, and socialist booksellers have already experienced such extralegal sanctioning."

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.[74] There is something deeply concerning here. Human well-being is simply not promoted by such employer meddling. Observing that employment is a voluntary arrangement doesn't change *that* fact. Similarly, observing that some sources of financial censorship are private doesn't mean they do no harm or that we oughtn't look for alternatives. 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 -- patronage, lobbying, loopholes, specialized regulations designed to curb competition, and so on -- it is not always easy to cleanly discern "private" from "state" censorship. Indeed, private firms often have little choice but to engage in financial censorship at the direction of a state.[75] 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.[76]

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, such as Black Lives Matter protesters… platforms' regulatory efforts often have weak due-process mechanisms, lack transparency and accountability measures, and can disproportionately stifle the speech of marginalized populations.[77]

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 intermediaries.[78] Banks, states, credit agencies, and so on

---

[74] See Anderson (2017): 39-40.

[75] Kesari et. al. (2017): 1123 describes Operation Chokepoint, in which the Obama-era Justice Department "targeted banks with subpoenas and investigative attention to determine whether they were aware of or were colluding in fraud perpetrated by partner payment providers. This investigatory attention caused banks to sever relationships with both questionable and lawful merchants…"

[76] Although the internet has a storied record of being used as an anti-censorship tool, states have also found it a convenient means of turning private actors into proxy censors; see Kriemer (2006): 14.

[77] Tusikov (2019): 51. Tusikov also cites Noble (2008) in this connection.

[78] Mann and Belzey (2005): 258 argue that the intermediaries eventually become indistinguishable from those lawmakers sought to regulate.

have the power to censor transactions between two parties because they stand between those parties.

5.4 Permissionless payments

It is one thing to point out expansive examples of financial censorship and observe the dangers they pose. But are there solutions? One might look here for public policy solutions. But such solutions will likely face steep resistance. For them to work, powerful authorities around the world would have to cede their perches atop the global financial system. So, as Hayek once observed, "...all we can do is by some sly, roundabout way introduce something that [government] can't stop."[79] We think the point applies to both governments *and* corporations.[80]

We need a new structure. Cryptocurrencies suggest one. How? Cryptocurrencies inhabit payment networks built to lack authorities.[81] They aim to be *permissionless*.[82] A completely permissionless payment network has no authorities -- no party to the network that can prevent or block transactions reliably. Not every payment network that aims to be permissionless achieves perfect permissionlessness. Some fail altogether. But the Bitcoin network in particular has achieved a relatively high degree of permissionlessness.[83]

---

[79] Quoted in Blanchard (1984). We are not the first to connect this particular remark of Hayek's to Bitcoin. See, e.g., O'Sullivan (2016): 95: "Bitcoin may just be that "sly, roundabout way" to force reform of the global monetary system".

[80]While earlier attempts at censorship-resistant digital cash were quickly quashed -- think here of Liberty Reserve or e-gold -- authorities have been much less successful in creating anything close to a coherent regulatory framework (punitive or otherwise) for cryptocurrencies. Perhaps this is because Bitcoin and its ilk are a unique and unexpected combination of existing technological and economic ideas. Luther (2020) documents the ways in which cryptocurrency regulations on the books are imprecise, internally incoherent, or selectively enforced.

[81] Cryptocurrencies that protect financial privacy offer another kind of solution to censorious authorities. It is costly (and in some cases, may be impossible) for states or firms to block individual transactions when the destination, source, and amount are unknown. With shielding and obscurity protections in place, cryptocurrencies force states or firms to attempt a *complete ban* on the entire payment network -- a ban that may be unworkable as a matter of politics or practical computer science. For a helpful and fascinating treatment of the economics of banning a given cryptocurrency, see Hendrickson and Luther (2017) and Hendrickson et. al. (2016).

[82] One important question is the precise extent to which cryptocurrencies make good on this promise. A number of factors suggest a mixed answer. Here are just three examples suggesting that Bitcoin is more centralized than it may first appear: (i) the Bitcoin network is maintained by large pools of miners, (ii) most users enter and exit the ecosystem through centralized exchanges, and (iii) most users use just a limited range of software to interact with the Bitcoin network. Each of these factors make for potential chokepoints: miners, exchanges, or software developers. For discussion, see Gervais et. al. (2014). In evaluating Bitcoin for permissionlessness, it is important to take into account the cost of developing workarounds to chokepoints. It is, for example, trivially easy to modify open-source Bitcoin software as one likes and thus be one's own bank. This workaround to potential software developer chokepoints (roughly, a few classes on coding, a computer, and internet access) is much less costly than, say, applying for one's own bank charter. Even though Bitcoin doesn't score *perfectly* on permissionlessness, it plainly does far better than legacy financial systems.

[83] We do not say, as many do, that cryptocurrencies are *trustless*. Storing or transferring significant amounts of value through a cryptocurrency clearly requires trust *of some kind*. One wouldn't do this

Gaining access to a cryptocurrency's network requires nothing but internet access and one of many free software applications. No registration is required, and the network doesn't need to know anything about you. With the internet and an app, anyone may construct a transaction and send it to the network. Then, without using authorities, a typical cryptocurrency network validates, settles, and clears the transaction.[84]

Many cryptocurrencies allow users to transfer value without trusting an authority to act responsibly. But their permissionlessness can extend beyond the realm of sending and receiving value. In Bitcoin and other cryptocurrencies, users together play the roles of banks and clearinghouses. The network as a whole validates, settles, and clears transactions instead of relying on authorities to do these jobs. 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. So a network like Bitcoin's takes the trust we normally place in a few authorities and spreads it thinly over the entire network.

5.5 Financial inclusion beyond payments

We've thus far explored the role of *payments* in permissioned financial networks. But these networks serve other purposes too, and similar considerations show a role for permissionless cryptocurrencies in *credit* and *banking*.

Credit is a vital avenue to wealth creation and accumulation. But it is not extended to all. One vivid American example is redlining, where the Federal Housing Administration refused to insure mortgage loans to people living in color-coded neighborhoods -- primarily lower-income Black people living in urban areas.[85] Exclusion from credit markets is economically devastating, so unsurprisingly, people seek credit elsewhere. Each year 12 million Americans take out a payday loan or car title loans, making it a multibillion dollar industry. The average loan is $375, and the average loanee pays $520 in interest.[86]

---

without some confidence that one wouldn't just lose it all. But note that the trust at issue here need not be directed at a central authority or institution (like a bank). Rather, the trust is directed at a *system* or the forces that produce desirable and predictable behavior from its various parties -- a system that is implemented, in turn, by the underlying code and the cryptographic structures it deploys. See Maurer et. al. (2013): 273-274 and Fama et. al. (2019): 188.

[84] How cryptocurrency networks transfer value without trusted intermediaries, and how the network achieves consensus in their absence about who has which amounts of value, are topics of the next section.

[85] The effects of this are still seen today, where Black families own 1% of the wealth in America today; they owned 0.5% in 1863 when the Emancipation Proclamation was signed. White families today have nearly 10 times the net worth of Black families and more than eight times that of Hispanic families. See Dettling et. al. (2017). For more on racial disparities here and their origins in access to credit, see Mitchell and Franco (2018) and Rothstein (2018).

[86] 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.

Many also suffer from poor access to banking. Small accounts aren't that profitable, and as a result, 22% of US households are unbanked. Unbanked people have to pay to cash their paychecks, to get money orders to pay their rent and other bills, to secure prepaid debit cards, and so on.[87] 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.[88]

Two problems, then: borrowing and banking. Cryptocurrency promises solutions to both. No bank account or permission is required to hold, receive, or send cryptocurrency. And 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 who can stake enough collateral in cryptocurrency can receive a loan.[89]

Cryptocurrencies democratize monetary value in much the same way the internet has democratized information. The internet provides an alternative and difficult-to-censor pathway for valuable information; similarly, cryptocurrencies provide an alternative and 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.[90] 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.[91] Similarly, although we recognize the new modes of wrongdoing cryptocurrencies enable, we expect the benefits of cryptocurrencies to outweigh their costs. Since cryptocurrency networks like Bitcoin's serve as a censorship-resistant payment system, many around the globe increasingly see them as a hedge and competitive check on traditional payment systems.[92] And, like the internet, we expect them to contribute to human flourishing.

6. Consensus

6.1 Consensus matters

Authorities that oversee electronic payment systems can engage in both surveillance and censorship. But they have these powers precisely because they are useful intermediaries. Not

[87] Recent analysis reveals a strong preference among fraudsters for stolen prepaid debit cards over credit cards; see Aliapoulios et. al. (2020). Unbanked individuals -- the target market for prepaid debit cards -- accordingly bear the brunt of such fraud.
[88] Pew (2012).
[89] For an argument to this effect with a focus on how Bitcoin in particular can help Black Americans, see Jackson (2019).
[90] Bridy (2015): 1523, 1563.
[91] See Nisbet et. al. (2012), Ruijgrok (2017), and Stoycheff and Nisbet (2014).
[92] For a vivid example of Bitcoin's censorship-resistance being used to buck Russian political authorities, see Baydakova (2020).

only do they settle accounts between parties who may not otherwise trust each other; they also protect the integrity of the overall financial system by ensuring that no one spends the very same money more than once. Although cryptocurrency networks eschew authorities, they still aim for the integrity that authorities provide. Since these networks lack authorities to issue top-down judgments about who has which amounts of value, they must achieve consensus concerning the ledger some other way. Bitcoin's own approach has inspired a number of alternatives. But consensus comes at a cost, and choosing one or another involves tradeoffs. In this section, we explain the two most influential designs and some difficulties prompted by each.[93]

6.2 Consensus machines: work and stake

Updating a ledger without authorities is tricky. Real value is at stake among parties whose interests needn't align. *You* may want the ledger to say that other participants have recently transmitted amounts to *your* address, while *those* participants would very much like to keep their amounts right where they are -- or both spend *and* keep them!

Coordination without authority is the goal here, and it has game-theoretic, economic, and political dimensions.[94] There are normative dimensions, too, and we'll now 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:[95]

> Proof of Work (PoW): miners compete to solve a mathematical puzzle that can only be solved by brute force (trying over and over again to arrive at a solution) -- or astonishingly good luck. Having *provably done some* -- and probably a certain amount -- of *computational work*, the winning miner may create the chain's next block of valid transactions.[96]
>
> Proof of Stake (PoS): validators may add a new block to the blockchain only upon demonstrating sufficient interest or *stake* in the blockchain and the value it stores -- by, for example, proving control over a sufficiently high amount of the cryptocurrency. Among the eligible validators, one may be selected at random or through some other means, and the winner may create the chain's next block of valid transactions.

[93] For a primer on the technical and game theoretic issues at stake in selecting a consensus mechanism, see Chowdhury (2020): Chapter 3.
[94] The question of who gets to decide how a ledger is to be updated can be thought of as a specification of one central question of political theory -- *who should rule?* For a spirited treatment of that question and its role in political theory, see Pickel (1989).
[95] For 28 other possible consensus procedures, see Racsko (2019): 358-359.
[96] On PoW blockchains as "trust machines" and the economics governing them, see Berg et. al. (2020).

By a long mile, PoW is the most popular consensus procedure, followed by PoS in a distant second place. Each involves difficult tradeoffs. We'll highlight a few.[97]

Bitcoin deploys PoW,[98] as do Zcash, Bitcoin Cash, Ethereum, and many others.[99] 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 succeeding may devalue their winnings, as discussed in Section 2.2.

PoW, however, uses a lot of electricity. A lot. Bitcoin presently uses 0.21% of the world's daily electricity -- about as much as Switzerland.[100] 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?[101]
- 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?[102]
- Does Bitcoin mining encourage more or less harmful ways of producing electricity?[103]

---

[97] We here call PoW and PoS "consensus procedures", although neither suffices on its own to reach consensus. PoW and PoS each protect against sybils, internet zombies which are cheap to create and could artificially inflate the vote for or against a version of the ledger. Bitcoin leverages the anti-sybil proof-of-work mechanism into a consensus procedure by requiring that the network vote for the version of the ledger with the most accumulated proof-of-work. The entire procedure is often labeled "Nakamoto consensus" and involves a novel solution to the Byzantine Generals Problem in computer science, a problem about how to achieve consensus without a central authority introduced in Pease et. al. (1980) and famously discussed in Lamport et. al. (1982).

[98] Strictly speaking, "Bitcoin's mining puzzle is not a true proof-of-work scheme but a probabilistic one. Finding a solution is computationally challenging on expectation, but it is possible to get lucky and find a solution with very little work." Bonneau et. al. (2015), p. 4 fn. 7. For a more technical but still readable description of Bitcoin mining and PoW, see Antonopoulos (2015): Chapter 8.

[99] Ethereum developers have promised a move towards Proof of Stake for years; it remains to be seen whether or how that move will unfold.

[100] Baraniuk (2019).

[101] Bitcoin is mostly powered by green/renewable energy. See Bendiksen and Gibbons (2019): 1, Vincent (2016), Carter (2020) and Harper (2019).

[102] Accurate assessments are not easy to come by here. But a quick comparison of Bitcoin's annual electricity costs (around $3 billion) to the Federal Reserve's annual budget ($4.7 billion) does not obviously support any decisive objection to Bitcoin's implementation of PoW. We've not included the proportion of the US military budget that serves to protect the dollar's status as the global reserve currency, the electricity use of commercial banks, the government and commercial banks of other countries, the resources used by private corporations around the world used to settle transactions, or the research, design, and implementation of anti-counterfeiting measures all over the world.

[103] There may even be positive effects from Bitcoin's energy use. Bendiksen and Gibbons (2019): 10 say, "Overall, our findings reaffirm our view that Bitcoin mining is acting as a global electricity buyer of last resort and therefore tends to cluster around comparatively under-utilised renewables infrastructure. This could help turn loss making renewables projects profitable and in time — as the industry matures and

Answers are by no means obvious. So it is unsurprising that some cryptocurrencies forego PoW. Other consensus protocols have arisen in reply to these staggering energy costs. 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.[104] 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.

Problems with PoS abound.[105] First: the rich get ever richer. The more currency you have, the more likely you are to get more. Although there are technical proposals for limiting this effect, the endgame here tends towards domination by a few early holders.[106] Second: in PoW currencies, miners have to choose a chain on which to mine, and they expend resources to mine on that chain. The incentives here discipline miners towards convergence, which enhances the network effects of the selected chains in terms of both adoption and security. For PoS currencies, there are few disincentives for working on multiple chains. But this distributes chain allegiance widely and could come at the price of both critical network effects that make adoption viable, and network speed. A final problem 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.

7. Monetary policy

Having surveyed two approaches to the question of how to find agreement on updating a ledger, we now turn to monetary policy and the injection of new amounts.[107]

---

settles as permanent in the public eye — could act as a driver of new renewables developments in locations that were previously uneconomical."

[104] And current PoS currencies don't typically reward the publisher of a block with new currency -- just transaction fees.

[105] For a convincing expression of some of these problems and comparison to Bitcoin's PoW, see Poelstra (2015). Davenport (2019) raises intriguing connections between PoS and tax law and argues that new amounts from staking should best be thought of as a penalty imposed on non-staking rather than as a reward for those who stake.

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

[107] We thus leave untouched important questions about the proper use or fairness of *pre-mining* -- assigning significant amounts of a new cryptocurrency to its creators upon its launch. The economic questions about Bitcoin and blockchains more generally raised in this section are by no means the only ones worth pursuing. For a useful sample, see Berg et. al. (2019), Catalini and Gans (2017), and Davidson et. al. (2018).

7.1 Inflation and money supply

Cryptocurrencies differ widely in monetary policy and issuance. Some have no provably strict issuance schedule at all and thus resemble a state-issued fiat currency with a discretionary supply.[108] Some follow a negative schedule: over time, their total supply declines.[109] Others follow a provably strict positive schedule of issuance: over time, their total supply increases.[110] As usual, Bitcoin deserves special interest. Its supply will eventually approach 21 million BTC.[111] What is notable is not that the total supply of BTC increases over time; many currencies do that. Instead, the supply increases at a declining rate and eventually *stops*.[112] In stark contrast to fiat currencies and commodity monies such as gold or silver, supply of new Bitcoin is inelastic[113] and not a function of demand for Bitcoin.[114]

Before considering arguments over whether the Bitcoin approach is advantageous, we'll introduce a standard analytical framework: the quantity theory of money.[115] This theory relates the supply of money (M), its velocity (V), the price of output goods and services (P), and the

[108] ETH, for example, which changed its supply schedule no fewer than six times from 2016-2020. See https://docs.ethhub.io/ethereum-basics/monetary-policy/

[109] BNB, for example, which began with a total supply of 200,000,000 but will eventually approach 100,000,000 after a series of quarterly and publicly verifiable "burns". These burns are not, it's worth noting, baked into the code, as it were; they unfold at the discretion of Binance, the creators of BNB. See https://whitepaper.io/coin/binance

[110] Peercoin, for example, has a theoretically unlimited money supply that is set to inflate (capped at a rate of 1% per year).

[111] This will happen upon the mining of block 6,930,000: on or around 2140CE. As Böhme et. al. (2015), explain, Bitcoin's issuance schedule has obvious antecedents in the monetarist thought of Milton Friedman: "In a broad sense, the Bitcoin economy implements a variant of Milton Friedman's… "k-percent rule"—that is, a proposal to fix the annual growth rate of the money supply to a fixed rate of growth. Indeed, Bitcoin's protocol calls for an end of the minting phase at which point k = 0. In fact, k may even be negative in the future, because bitcoins can be irreversibly destroyed when users forget their private key."

[112] Bitcoin thus resists easy classification in traditional economic categories. Even if it is or could be money, it is neither a fiat money (its supply cannot be easily manipulated by an issuer) nor a commodity money (it has little intrinsic value or non-monetary use). Selgin (2015), accordingly, argues that Bitcoin is a *synthetic commodity*. Bjerg (2016) sees Bitcoin as a new form of money that combines aspects of commodity money, fiat money, and credit money, resulting in something that is "the worst form of money, except for all the others".

[113] See Norland and Putnam (2019: 81-82) on the certainty of supply and perfect inelasticity of Bitcoin. On cryptocurrencies as *bubble* assets, see Chaim and Laurini (2019), and especially Cagli (2019).

[114] Nakamoto (2008: 4) compares Bitcoin supply to that of gold, and notes one dissimilarity -- Bitcoin's supply barely responds to demand, whereas gold's significant elasticity in supply is in part a function of its demand; for more, see Cachanosky (2019): 371. For further analysis that locates Bitcoin as somewhere *between* the US Dollar and gold, see Dyhrberg (2016) and Klein et. al. (2018).

[115] This framework and the real/nominal variable distinction on which it relies (Y is, for example, real and so specified in physical units such as *guitars produced*; P, by contrast, is nominal and so specified in arbitrary monetary units such as *dollars*) derive from Hume and other classical economists. One helpful historical treatment is in Evans and Thorpe (2013).

amount of output (*Y*) thus:

$$MV = PY$$

Where *V* and *Y* are invariant, any increase in *M* will result in an increase in *P* -- a general rise in or inflation of prices.[116] This is the condition of most state-issued fiat currencies; they tend to increase in supply and thus engender inflation. Where *M* and *V* are invariant, any increase in *Y* will result in a decrease in *P* -- a general decrease in or deflation of prices.[117] Under conditions of real economic growth, that is (when real outputs -- *Y* -- rise), standard economic wisdom predicts deflation of prices from a Bitcoin-style issuance schedule. In general, a driving factor behind either inflation or deflation is the supply of money.[118]

Since Bitcoin has such a distinctive approach to money supply, which is in turn so closely connected to inflation or deflation, one naturally wonders which is better, and for whom. This is the proxy question by which we'll investigate whether Bitcoin-style monetary policy improves over state-issued fiat currencies and, accordingly, whether it would be *good* for Bitcoin (or some other cryptocurrency) to be used as money.

7.2 Stateless money

We've introduced a substantive question about monetary policy: should it tend towards inflation, or deflation, or what? A procedural question also lurks nearby. *Who*, if anyone is to oversee all this? Bitcoin's full answer here resists easy classification. But this much is clear: it assigns no essential oversight role to the state.

Money without state is controversial, to put the point mildly. Economists agree more often than do philosophers -- but not by much. So it is striking to observe the orthodox status of the view that issuing money is a critical state function.[119] The standard argument for orthodoxy is simple. Powerful market forces engender the creation of too much money. If Schrute Bucks have any value at all, Dwight has an incentive to print more. The incentive remains until the value of a

---

[116] The *ceteris paribus* condition can be surprisingly realistic. The velocity of money (i.e. the rate at which money changes hands) is largely a function of factors other than money supply (how many dollar bills are in circulation plays a negligible role in output when compared to, for example, the availability of natural resources or capital). See Friedman and Schwartz (1963).

[117] For vividness, consider the outcome of increasing the right-hand denominator in this algebraic variation of our target equation: $P = MV/Y$.

[118] So Mankiw (2018): 632, "According to the quantity theory, the quantity of money available in an economy determines the value of money, and growth in the quantity of money is the primary cause of inflation. As economist Milton Friedman once put it, 'Inflation is always and everywhere a monetary phenomenon.'" The view expressed here is *strict* monetarism. The view that money supply is a dominant but not unique factor in inflation -- *loose* monetarism, we might call it -- is widely accepted across economics even by those who'd deny Friedman's strong formulation.

[119] So Klein (1974): 423: "Few areas of economic activity can claim as long and unanimous a record of agreement on the appropriateness of governmental intervention as the supply of money... The monetary role of government is agreed to include, at a minimum, the monopolistic supply of a currency, into which all privately supplied demand deposits should be convertible."

Schrute Buck equals the marginal cost of printing a new Schrute Buck.[120] This result holds even if Stanley is printing Stanley Nickels too; competition between private issuers is no solution. What is needed, says orthodoxy, is a currency issued by an actor that responds to *other* incentives (political forces and elections, for example), which prevents over-issuance.[121]

There is some irony here. State-issued currencies are not obviously immune to over-issuance, for one.[122] Bitcoin, furthermore, is provably free of such over-issuance, by design. Bitcoin's architecture answers a standard objection to privately issued currency.[123]

7.3 Standard inflation arguments

What can be said in favor of Bitcoin's approach? Proponents advance a family of arguments:

> Inflation -- a general rise in prices as denominated in a target currency -- is equivalent to a drop in purchasing power of that currency. This loss in purchasing power is a sort of covert tax imposed on those who hold the currency. And inflation is, or is generally caused by,[124] an increase in the supply of money, typically a state-issued fiat currency. This is a *problem*. The plain *solution* is a currency that *cannot* increase in total supply -- or, at least, can only increase along a fixed schedule that is not subject to political machinations or capricious manipulation. Cryptocurrencies -- some of them, at least -- fit that bill and it is therefore good that they be used as money.[125]

---

[120] See Friedman (1960): 6-8 and Mafi-Kreft (2003): 475.

[121] For a counterargument according to which the *reputation* of an issuer, given a commitment to a particular money supply, can contribute to a monetary equilibrium without overissuance, see Araujo and Camargo (2008). What's interesting for our purposes is that Bitcoin appears to involve just such a commitment: miners issuing BTC thereby commit to BTC over, say, ZEC.

[122] Federal Reserve Economic Data, for example, reports one measure of monetary base (in millions of USD) as 50,058 in May 1959 and 4,844,940 in April 2020. This vastly outstrips the growth in real USD GDP over the same interval (from 3,121.936 to 18,974.702, also in millions of USD). See https://fred.stlouisfed.org/series/BOGMBASE and https://fred.stlouisfed.org/series/GDPC1

[123] Martin and Schreft (2006) anticipate this advantage of Bitcoin to some degree; they show that there is no tendency towards overissuance provided that "agents believe that if an issuer produces more than some threshold number of notes, then only those notes issued up to the threshold will be valued; additional notes will be worthless.".

[124] A minority of economists -- namely, those hailing from the so-called Austrian school -- will insist on the former; they take a rise in money supply to be *constitutive* of inflation and diagnose a general rise in prices as a mere effect of that underlying condition. More mainstream views characterize inflation as a general rise in prices. We suspect that the apparent disagreement here is merely verbal and simply reflects that the word "inflation" is polysemous. Note, though, that substantive disagreements are close at hand: Austrians and more mainstream economists will disagree on both the correct antidote to bad inflation and the correct diagnosis of its causes (which could in some cases include factors beyond money supply -- factors such as V or Y, that is).

[125] Non-academic or popular defenders of arguments along these lines number in the thousands -- maybe more. For a small sampling of such, one need only Google for expressions like "Bitcoin and inflation". It is harder to find serious academic statements of the arguments in view. But one influential source is Ammous (2018b): Ch. 4. Below, we'll separate the broad argument at hand into various strands. It is hard, we note, to overestimate the importance of arguments along these lines, despite the fact that they do not

What's to say? The framework introduced above, to some degree, vindicates one key assumption. A general rise in *M* will tend towards inflation of *P*, which is indeed equivalent to a drop in purchasing power of the currency.[126] But whether such a drop is *bad* strays into normative and philosophical domains well beyond positive economics. Proponents of standard inflation arguments typically identify one (or more) of five problems with inflation: inflation entails a loss in purchasing power, inflation is a tax, inflation is hidden, inflation is subject to capricious political processes, or inflation penalises savings or investment over consumption.[127]

A full evaluation of these five claims is beyond our present ambitions.[128] But it's instructive to note significant weaknesses in each.

On loss of purchasing power: inflation does indeed involve a loss in *nominal* purchasing power. But it need not involve any loss in *real* purchasing power (to confuse these is to commit "The Inflation Fallacy"). For a rise in price paid by buyers entails a rise in receipts by sellers; nominal incomes, accordingly, rise with nominal prices.[129] Put just a little more simply: inflation means that your dollars are worth less, sure. But it also means you'll be paid more dollars when selling goods or labor. There needn't be any *real* loss here.[130]

On inflation as taxation *per se*: many cryptocurrency proponents explicitly endorse anarchist political theories.[131] Their arguments, if sound, tell against any state at all -- including taxation

---

fall squarely within mainstream economic opinion. The popularity of these arguments and their departure -- for good or for ill -- from mainstream economic thinking is aptly summarized in Malherbe, et. al. (2019), 149.

[126] This drop is only nominal, and need not result in any real loss, as we'll see shortly.

[127] See Maurer et. al. (2013): 270 and O'Sullivan (2016): 93-94.

[128] These are not the only alleged harms of inflation, to be sure. Others include menu costs (the inconvenience of updating nominal prices), shoeleather costs (the inconvenience of maintaining reduced stores of money than one otherwise would), inefficiencies in tax treatment of interest income. These are all well-understood and accepted by mainstream economists as genuine downsides to inflation. Proponents of standard inflation arguments for cryptocurrency adoption, interestingly, rarely appeal to *these* considerations but instead rely on the first five noted in the main text.

[129] Under inflation, even nominal incomes for individuals on "fixed" income benefits tend to rise, since benefits are typically indexed to inflation. See Burdick and Fisher (2007).

[130] A wrinkle: new supplies of money have to appear *somewhere*, and there's no guarantee that rise in prices will percolate outwards in a uniform or expeditious way. One result can be a redistribution of buying power towards those who are closest to the supply of new money (those who sell debt purchased with new money, for example). The classic study of this effect is Cantillon (1755/1959). Reflection on this effect supports, we think, a rather *different* argument -- inflation isn't bad because it kills purchasing power, but because it redistributes it. We discuss the point further, below.

[131] For extensive documentation, see all of Golumbia (2016), but especially Chapters 1-2. Golumbia claims that the ideological foundations of Bitcoin and other cryptocurrencies stem from the political far-right. This claim, we think, underplays the role of Austrian Economics in the emergence of Bitcoin and cryptocurrencies in general. Proponents of the Austrian school, we note, tend to be avowed opponents of far-right regimes and ideas. A controlling theme of Hayek (1944), for example, is that growing state power may facilitate a slide towards the horrors of national socialism in the German mold. The ideology here is not aptly characterized as far-right, then. Nor would it be accurate to think of it as strictly or even mainly

imposed by inflationary monetary policy. In reply, though, we note that these arguments are not available or convincing to the vast majority of political theorists or philosophers, most of whom think that at least some state taxation is justified. A convincing argument here would need to show that there is some *special* feature of "taxation by inflation" -- one not exemplified by all taxation or state action as such -- by virtue of which it is wrong or bad.[132]

On inflation as a hidden tax: although many taxes are hidden from those who ultimately pay them, they're not obviously bad or harmful for that reason.[133] And inflation, furthermore, isn't all that hidden: everyone knows that a candy bar used to cost a nickel.[134]

On inflation and politics: cryptocurrencies, too, are subject to politics. One need not look far -- miners, developers, users, and advocates of cryptocurrencies are notoriously cantankerous, and routinely "fork" projects over disagreements both substantive and petty. That there are some market pressures here doesn't make the space an *obvious* improvement over, say, using interest rates or quantitative easing to manipulate public opinion before an election.[135]

On penalizing savings or investment: it may be bad to penalize savings or investment. But it is also bad, and perhaps worse, to penalize *consumption*, as is the case with a disinflationary or deflationary currency in circumstances of real productivity growth.[136]

"anti-government". Proponents of cryptocurrencies tend to be suspicious of institutional overreach of *any* kind whether from states or private firms. For an argument that Bitcoin is, in fact, well-suited for achieving egalitarian ideals extending even to left-wing socialism, see Huckle and White (2016).

[132] Another wrinkle in the argument is that *direct* funding of state spending through monetary base expansion -- something that can be aptly characterized as a tax -- is not prevalent. It is unclear whether more widely used procedures for monetary base expansion that ripple outwards indirectly (as when a central bank purchases bonds or securities) should count as a *tax* at all.

[133] Taxes on labor income, for example, are ultimately borne by consumers rather than hiring firms.

[134] It may be useful here to distinguish two important questions; a convincing assessment of the hidden tax argument would address both. One is the extent to which the hiddenness of a tax affects behavior (whether of those who pay it or those who impose it). This is largely a matter of positive economics. A second question concerns whether hidden taxes are compatible with ideals concerning, e.g., democratic rule or transparency. This is largely a matter of political theory or political philosophy.

[135] Some of Bitcoin's features are more easily subject to social and political forces than are others. The one feature that is perhaps *most* resistant to any change at all is the supply schedule. Even forks of Bitcoin that make changes to, for example, scaling solutions tend to keep intact the fixed supply schedule. There is much more to say here on the social and political forces at play. See Dodd (2018), Hayes (2019), and, especially, DuPont (2019): Chapter 8.

[136] Mainstream (and Keynes-influenced) economic opinion suggests it is at least equally as bad to penalize consumption as savings or consumption. See, e.g., discussion of the "paradox of thrift" in Samuelson and Nordhaus (2010): 452. For a heterodox alternative that in fact pre-dates Keynes, see Hayek (1929). As before, the $MV = PY$ framework is helpful. A rise in Y predicts a drop in P, if M and V are held constant, which in turn provides an incentive for consumers to *withhold* spending -- why buy a phone for $1,000 today when it will only cost $950 tomorrow? The effect here is most pronounced for goods with highly elastic demand.

We don't claim that all five claims decisively fail. But they face serious impediments.[137] Are there *better* ways to advance a Bitcoin-style monetary policy? We think so. Here are three:

First, the problem with inflation is not that it happens, or even that it is too high. Predictable inflation can be hedged against.[138] The problem is when it is *unpredictable*. Bitcoin's supply, by contrast, is utterly predictable. Indeed, Bitcoin can be seen as the limit case or fulfillment of the monetarist ambitions of a fixed and modest growth in money supply or of an algorithmically determined supply schedule.[139]

Second, inflation disproportionately rewards those who take on nominal debt. Inflation is a redistribution program.[140] This might be unobjectionable -- if it turned out to favor the least well-off, for example. But it doesn't. It favors, instead, those who have significant debt denominated in that currency.[141] And that's a select group within the wealthiest countries -- and those wealthy countries themselves.[142] Inflation is a debt-forgiveness program for the global rich.[143]

Third, inflation begets inflation. This is no secret.[144] And it is precisely the *risk* of inflationary spirals that leads central banks to monitor economic indicators for signs of inflation and then adjust policy in their light. But institutions -- and central banks are no exception -- tend to do best when subject to competitive checks.[145] Alternative state-issued fiat currencies are one such check. Were the US dollar to collapse under bad management, the world would quickly adopt

---

[137] All five, we note, fall pretty far outside of professional consensus among economists, for roughly the reasons we've cited in the main text. Shiller (1997) surveyed the population at large and professional economists. For the US population as a whole, 52% fully agreed that preventing high inflation was a very important national priority, compared to 18% of economists, and just 4% completely disagreed compared to 18% of economists. See the discussion of this in the popular macroeconomics textbook *OpenStax* (2020): Chapter 9.4.

[138] Some US Treasury bonds (Treasury inflation-protected securities, or "TIPS"), for example, are indexed to inflation.

[139] What we say here about predictable supply is compatible, of course, with variation deriving from individual decisions to sell, which decisions would increase the supply of Bitcoin available for purchase on a given market. Despite such variation, the aggregate stock of Bitcoin that *exists at all, whether for sale or not* is strictly predictable and limited.

[140] Brennan and Buchanan (1981).

[141] For more connections between central banking and monetary policies that exacerbate inequality along these lines, see Fontan et. al. (2016).

[142] Doepke and Schneider (2006).

[143] The Cantillon effect, also discussed above, is relevant here as well and suggests another way in which inflation redistributes. The global rich don't just hold a lot of debt; they are also "closest to the money spigot", and benefit disproportionately from that proximity. For further discussion in connection with the ethics of inflationary monetary policy, see Bagus et. al. (2014).

[144] There's even a term for this phenomenon: an *inflationary spiral*. See Black et. al. (2012).

[145] The *locus classicus* for currency competition and its positive effects is Hayek (1976), which notoriously advocates for the total *privatization* of money. Backhouse (2006) locates Hayek's views on money within his broader economic thought. Selgin and White (1994) offer the canonical development of Hayek's "free banking" model. For a useful overview of historical objections to Hayek, see Ferris and Galbraith (2006).

alternatives.[146] Non-state-issued alternatives like cryptocurrencies provide another competitive check. Their existence incentivizes policy-makers to behave responsibly.[147]

We've surveyed eight arguments purporting to show significant advantages to Bitcoin-style monetary policy. We find the first five unconvincing, but the latter three may yet succeed. And if that's right, then we've made some progress towards a positive answer to our normative question: *yes, it is good to use cryptocurrency as money, because doing so promotes sound monetary policy*.[148]

8. Conclusion

Supposing that a cryptocurrency *could* fill key money roles, would it be all things considered *good* for it to do so?[149] Two themes emerge in our discussion. First, there are a range of considerations that support a positive answer. There is a plausible (though perhaps not decisive) case that cryptocurrencies can promote goods like privacy, financial inclusion, and sound monetary policy. Second, a responsible treatment of the issues requires a mixed approach that integrates techniques, ideas, and results from philosophy, politics, and economics.

---

[146] For a useful but dated overview, see Cesarano (1999). See also Halaburda and Sarvary (2016): 32-46. Endres (2009) argues that competition between state-issued currencies provides a sufficient check without any need for privatization of money. On "currency wars" in general -- i.e., the use of monetary policy for strategic geopolitical purposes and the general phenomenon of competition across state-issued currencies -- see Forrest, Ying, and Gong (2018).

[147] Fernández-Villaverde (2018) argues that cryptocurrencies will deliver neither price stability nor optimal money supply but can nonetheless -- through competitive pressure -- discipline central banks towards optimal monetary policy. See also Fernández-Villaverde and Sanches (2018). For cautionary notes, see Berentsen (2006) and Rahman (2018). Importantly, the check provided here goes beyond any imposed by digital fiat currencies, which aren't likely to be helpful in this connection; see Kirkby (2018). One key asymmetry is that the cryptographic features of, for example, Bitcoin allow users to test and verify claims about supply and distribution for themselves.

[148] The final point about competition between currencies can be abstracted and strengthened. Perhaps inflationary currencies are good; perhaps not. But note: the widespread availability of alternatives -- cryptocurrencies are a fine example -- provides an important competitive check against *any* monetary policy. One could endorse a pro-cryptocurrency argument here, then, even while remaining strictly agnostic about an optimal supply schedule. What matters is that the availability of alternative cryptocurrencies provides policy-makers strong incentives to do well. For arguments that could be used to support reasoning along these lines, see Salter and Luther (2019), which argues that central bankers exhibit behavior that is adaptive. For more discussion of the claims at hand -- that competition tends to engender sound monetary policy, and so on -- see Mafi-Kreft (2003).

[149] The question as phrased is about what is *good*. But in further research it may be helpful to consider a related question about what is *right*, as well: should we treat a target cryptocurrency as money? Should you? The answer will depend, in part, on what you find valuable. The main arguments of this paper suggest that a positive answer is appropriate for individuals and firms that prize financial privacy, censorship-resistance, or sound monetary policy. Of course, there are still significant practical barriers to adoption, even in the face of arguments like this. On network effects and the barriers they pose to adoption, see Luther (2016a). On the critical role of *coordination* here, see Luther (2013) for an empirical case study and Luther (2018b) for a more theoretical treatment with an eye towards cryptocurrency adoption.

References

Abel, Andrew B., Ben S. Bernanke, and Dean Croushore (2008). *Macroeconomics*, 3rd ed. Boston: Pearson.

Albrecht, Chad and Steven Hawkins & Kristopher McKay Duffin (2020). "Legitimizing Bitcoin as a Currency and Store of Value: Using Discrete Monetary Units to Consolidate Value and Drive Market Growth" *Ledger*: 1-10. doi: 10.5915/LEDGER.2020.167

Aliapoulios, Maxwell, and Cameron Ballard, Rasika Bhalerao, Tobias Lauinger, & Damon McCoy (2020). "Swiped: Analyzing Ground-truth Data of a Marketplace for Stolen Debit and Credit Cards". Working paper. Available online: https://krebsonsecurity.com/wp-content/uploads/2020/07/nyu-cardshop.pdf

Ammous, Saifedean (2018a). "Can cryptocurrencies fulfil the functions of money?" *The Quarterly Review of Economics* 70: 38-51.

Ammous, Saifedean (2018b). *The Bitcoin Standard*. Hoboken, NJ: Wiley.

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

Anderson, Elizabeth (2017). *Private Government*. Princeton University Press.

Androulaki, Elli and Ghassan O. Karame (2014). "Hiding Transaction Amounts and Balances in Bitcoin" in *Trust and Trustworthy Computing* (Holz and Ioannidis, Eds), 161-178. Springer.

Antonopoulos, Andreas M. (2015). *Mastering Bitcoin*. Cambridge: O'Reilly.

Ballantyne, Nathan (2019). *Knowing Our Limits*. Oxford: Oxford University Press.

Baradaran, Mehrsa (2015). *How the Other Half Banks: Exclusion, Exploitation, and the Threat to Democracy*. Cambridge: Harvard University Press.

Baradaran, Mehrsa (2017). *The Color of Money: Black Banks and the Racial Wealth Gap*. Cambridge: Harvard University Press.

Baradaran, Mehrsa (forthcoming). "Banking On Democracy." Washington University Law Review.

Backhouse, Roger E. (2006). "Hayek on money and the business cycle" in *The Cambridge Companion to Hayek* (Edward Feser, ed): 34-50.

Bagus, Philipp and David Howden & Amadeus Gabriel (2014). "Causes and Consequences of Inflation" *Business and Society Review* 119, 4: 497–517.

Bailey, Andrew M. (2020). "Of all trades". Blog post: http://andrewmbailey.com/ofalltrades/

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

Baur, Dirk and KiHoon Hong and Adrian D. Lee (2018). "Bitcoin: medium of exchange or speculative assets?" *Journal of International Financial Markets, Institutions and Money* 54: 177-189.

Baydakova, Anna (2020). "Russian Activists Use Bitcoin, and the Kremlin Doesn't Like It" Coindesk. Available online: https://www.coindesk.com/russian-activists-use-crypto-kremlin-doesnt-like-it

Bendiksen, Christopher and Samuel Gibbons (2019). "The Bitcoin Mining Network" CoinShares Research. Available online: https://coinshares.com/assets/resources/Research/bitcoin-mining-network-december-2019.pdf

Benson, Carol Coye and Shaun Loftesness & Russ Jones. (2017). *Payments Systems in the US: A Guide for the Payments Professional*. 3rd Edition. Glenbrook Partners.

Berentsen, Aleksander (2006). "On the private provision of fiat currency" *European Economic Review* 50: 1683-1698.

Berg, Chris (2018). "Financial Privacy" in *The Classical Liberal Case for Privacy in a World of Surveillance and Technological Change*". Palgrave Macmillan.

Berg, Chris, and Sinclair Davidson & Jason Potts (2019). *Understanding the Blockchain Economy: An Introduction to Institutional Cryptoeconomics*. Cheltenham: Edward Elgar Publishing

Berg, Chris, and Sinclair Davidson & Jason Potts (2020). "Proof of Work as a Three-Sided Market" *Frontiers in Blockchain* 3, 2: 1-5.

Biryukov, Alex and Sergei Tikhomirov (2019). "Security and privacy of mobile wallet users in Bitcoin, Dash, Monero, and Zcash" *Pervasive and Mobile Computing* 59: 1-11.

Bjerg, Ole (2015). "How is Bitcoin money?" *Theory, Culture and Society* 33:53-72.

Black, John and Nigar Hashimzade & Gareth Myles (2012). "Inflationary Spiral" in *A Dictionary of Economics* (4th ed, Black, Hashimzade, and Myles, Eds). Oxford: Oxford University Press.

Blanchard, James (1984). Interview with F.A. Hayek. Available online: https://www.youtube.com/watch?v=EYhEDxFwFRU

Blanchette, Jean-François (2012). *Burdens of Proof: Cryptographic Culture and Evidence Law in the Age of Electronic Documents*. MIT Press.

Bohannon, John (2016). "The Bitcoin Busts" *Science Magazine* 351: 1144-1146.

Bonneau, Jospeph and Andrew Miller, Jeremy Clark, Arvind Narayana, Joshua A. Kroll, & Edward W. Felton (2015). "SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies" *IEEE Symposium on Security and Privacy*. DOI 10.1109/SP.2015.14

Brennan, H. Geoffrey and James M. Buchanan (1981). *Monopoly in Money and Inflation*. London: Institute of Economic Affairs.

Bridy, Annemarie (2015). "Internet Payment Blockades" Florida Law Review 67, 5: 1523-1568.

Brito, Jerry and Andrea Castillo (2013). *Bitcoin: A Primer for Policymakers*. Arlington: Mercatus Center.

Brito, Jerry (2019), "The Case for Electronic Cash: Why Private Peer-to-Peer Payments are Essential to an Open Society," *Coin Center Report*.

Brooke, Siân and Carissa Véliz (2020). "Views on Privacy: A Survey" in *Data, Privacy, and the Individual*. Available online: https://docs.ie.edu/cgc/research/data-privacy/CGC-Data-Privacy-and-the-Individual-Report.pdf

Brunton, Finn (2019). *Digital Cash: The Unknown History of the Anarchists, Utopians, and Technologists Who Build Cryptocurrency*. Princeton University Press.

Burdick, Clark and Lynn Fisher (2007). "Social Security Cost-of-Living Adjustments and the Consumer Price Index" *Social Security Bulletin* 67, 3.

Cagli, Efe Calgar (2019). "Explosive behavior in the prices of Bitcoin and altcoins" *Finance Research Letters*, 29: 398-403.

Cantillon, Richard (1755/1959). *Essay on the Nature of Trade in General*. H. Higgs, trans. London: Frank Cass.

Carter, Nic (2019). "It's the settlement assurances, stupid" Block post. Available online: https://medium.com/@nic__carter/its-the-settlement-assurances-stupid-5dcd1c3f4e41

Carter, Nic (2020). "The Last Word on Bitcoin's Energy Consumption". Coindesk. Available online: https://www.coindesk.com/the-last-word-on-bitcoins-energy-consumption

Carter, Nic and Bradley Rettler & Craig Warmke (manuscript). "Chain splits."

Catalini, Christian, and Joshua S. Gans (2017). "Some Simple Economics of the Blockchain" MIT Sloan Research Paper No. 5191-16. Available online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2874598

Chaim, Pedro and Márcio P. Laurini (2019). "Is Bitcoin a bubble?" *Physica* A 517: 222–232.

Chevalier, Michel (1854). *La Monnaie*. Brussels: Meline, Cans et Compagnie.

Chowdhury, Niaz (2020). *Inside Blockchain, Bitcoin and Cryptocurrencies*. CRC Press (Taylor & Francis).

Cowen, Nick (2020). "Markets for Rules: The Promise and Peril of Blockchain Distributed Governance" *Journal of Entrepreneurship and Public Policy*. http://dx.doi.org/10.2139/ssrn.3223728

Davenport, Ben (2019). "A Stake to the Heart". Available online: https://medium.com/@bendavenport/a-stake-to-the-heart-57fcd8ec323b

Davidson, Sinclair, and Primavera de Filippi, & Jason Potts (2018). "Blockchains and the economic institutions of capitalism" *Journal of Institutional Economics* 14, 4: 639–58.

DeCew, Judith (2018). "Privacy", The Stanford Encyclopedia of Philosophy (Spring 2018 Edition), Edward N. Zalta (ed.), URL = <https://plato.stanford.edu/archives/spr2018/entries/privacy/>.

Dettling, Lisa J. and Joanne W. Hsu, Lindsay Jacobs, Kevin B. Moore, & Jeffrey P. Thompson (2017). "Recent Trends in Wealth-Holding by Race and Ethnicity: Evidence from the Survey of Consumer Finances". FEDS Notes. Available online: 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, Claus and Peter Seele (2016). "Cryptocurrencies and business ethics" *Journal of Business Ethics* 152: 1-14.

Dodd, Nigel (2018). "The Social Life of Bitcoin" *Theory, Culture, and Society* 35, 3: 35-56.

Doepke, Matthias and Martin Schneider (2006). "Inflation and the Redistribution of Nominal Wealth" *Journal of Political Economy* 11, 6: 1069-1097.

Dotson, Kristie (2012). "How is this paper philosophy?" *Comparative Philosophy* 3, 1: 3-29.

Dyhrberg, Anne (2016). "Bitcoin, gold and the dollar" *Finance Research Letters* 16: 85-92.

DuPont, Quinn (2019). *Cryptocurrency and Blockchains*. Polity Press.
England, Catherine and Craig Fratrik (2018). "Where to Bitcoin?" *The Journal of Private Enterprise* 33, 1: 9-30.
Evans, Anthony J. and Robert Thorpe (2013). "The (quantity) theory of money and credit" *Review of Austrian Economics* 26: 463-481.
Fama, Marco and Andrea Fumagalli & Stefano Lucarelli (2019). "Cryptocurrencies, Monetary Policy, and New Forms of Monetary Sovereignty", *International Journal of Political Economy* 48: 174-194.
Fernández-Villaverde and Daniel Sanches (2019). "Can cryptocurrency competition work?" *Journal of Monetary Economics* 106: 1-15.
Ferris, J. Stephen and John A. Gailbraith (2006). "On Hayek's denationalization of money, free banking and inflation targeting" *The European Journal of the History of Economic Thought* 13:2: 213-231.
Flitter, Emily (2020). "'Banking While Black': How Cashing a Check Can Be a Minefield". *New York Times* (June 18). Available online: https://www.nytimes.com/2020/06/18/business/banks-black-customers-racism.html
Fontan, Clément, François Claveau, and Peter Dietsch, 2016, "Central Banking and Inequalities: Taking off the Blinders" *Politics, Philosophy & Economics* 15(4): 319–357.
Forrest, Jeffrey Yi-Lin and Yiron Ying and Zaiwu Gong (2018). *Currency Wars: Offense and Defense through Systematic Thinking*. Springer.
Frisby, Dominic (2014). *Bitcoin: The Future of Money?* Unbound.
Fridman, Milton and Anna Schwartz (1963). *A Monetary History of the United States*. Princeton: Princeton University Press.
Froomkin, A. Michael (1996). "The Essential Role of Trusted Third Parties in Electronic Commerce" 75 Or. L. Rev. 49.
Gervais, Arthur, Ghassan O. Karame, Vedran Čapkun, & Srdjan Čapkun (2014). "Is Bitcoin a Decentralized Currency?" *IEEE Security and Privacy*. 12, 3: 54-60.
Golumbia, David (2016). *The Politics of Bitcoin: Software as Right-Wing Extremism*. Minneapolis: University of Minnesota Press.
Harper, Colin (2019). "Oil Field Alchemy: How Bitcoin Can Turn Waste, Emissions Into Proof-Of-Work" Bitcoin Magazine. Available online: https://bitcoinmagazine.com/articles/oil-field-alchemy-how-bitcoin-can-turn-waste-emissions-proof-work
Harris, Joseph (1757). *An Essay Upon Money and Coins*. London: G. Hawkins.
Hayek, F.A. (1929). "The 'Paradox' of Saving" in *Prices and Production and Other Works: F.A. Hayek on Money, the Business Cycle, and the Gold Standard* (Salerno, ed.). Auburn: Ludwig von Mises Institute.
Hayek, F.A. (1944). *The Road to Serfdom*. London: Routledge.
Hayek, F.A. (1976). *Denationalisation of Money*. Institute of Economic Affairs.
Hayes, Adam (2019). "The Socio-Technological Lives of Bitcoin" *Theory, Culture, and Society* 36, 4: 49-72.
Hazlett, Peter K. and William J. Luther (2019). "Is bitcoin money? And what that means" *The Quarterly Review of Economics and Finance*.

Hendrickson, Joshua R. and William J. Luther (2017). "Banning bitcoin" *Journal of Economic Behavior & Organization* 141 (2017) 188–195.

Hendrickson, Joshua R., Thomas L. Hogan, and William J. Luther (2016). "The Political Economy of Bitcoin" *Economic Inquiry* 54, 2: 925-939.

Herskind, L., Katsikouli, P., & Dragoni, N. (2020). "Privacy and Cryptocurrencies - A Systematic Literature Review" *IEEE Access*, 8, 54044-54059. [9036864]. https://doi.org/10.1109/ACCESS.2020.2980950

Huckle, Steve and Martin White (2016). "Socialism and the Blockchain" *Future Internet* 8, 49.

Ince, Darrel (ed.) 2013. *A Dictionary of the Internet* (3rd ed). Oxford University Press.

Jackson, Isaiah (2019). *Bitcoin and Black America*. Independently Published.

Jevons, William Stanley. (1875). *Money and the Mechanism of Exchange*. New York: D. Appleton and Co.

Kahn, Charles M. And James McAndrews & William Roberds (2005). "Money is Privacy" *International Economic Review* 46, 2: 377-399.

Kayyali, Dia and Rainey Reitman (2014). "The Morality Police in Your Checking Account: Chase Bank Shuts Down Accounts of Adult Entertainers" Electronic Frontier Foundation. Available online: https://www.eff.org/deeplinks/2014/04/moral-police-your-checking-account-chase-bank-shuts-down-accounts-adult

Kesari, Aniket and Chris Jay Hoofnagle and Damon McCoy (2017). "Deterring Cybercrime: Focus on Intermediaries" 32(3) *Berkeley Technology Law Journal*.

Kirkby, Robert (2018). "Cryptocurrencies Cryptocurrencies and Digital Fiat Currencies" *The Australian Economic Review* 51, 4: 527–539.

Kiyotaki, Nobuhiro and Randall Wright (1989). "On Money as a Medium of Exchange" *Journal of Political Economy* 97, 4, 927-954.

Klein, Benjamin (1974). "The Competitive Supply of Money" *Journal of Money, Credit and Banking* 6, 4: 423-453.

Klein, Tony and Hien Pham Thu & Thomas Walther (2018). "Bitcoin is not the New Gold – A comparison of volatility, correlation, and portfolio performance" *International Review of Financial Analysis* 59: 105–116.

Kreimer, Seth F. (2006). "Censorship by Proxy: The First Amendment, Internet Intermediaries, and the Problem of the Weakest Link", 155 U. PA. L. REV. 11, 14.

Kubát, Max (2015). "Virtual Currency Bitcoin in the Scope of Money Definition and Store of Value" *Procedia Economics and Finance*, 30, 409–416.

Kumar, Raynil and Shaun O'Brien (2019). "2019 Findings from the Diary of Consumer Payment Choice". Fednotes/Federal Reserve Bank of San Francisco. Available online: https://www.frbsf.org/cash/publications/fed-notes/#2018

Kwecka, Zbigniew and William Buchanan, Burkhard Schafer & Judith Rauhofer (2014). "'I am Spartacus': Privacy enhancing technologies, collaborative obfuscation and privacy as a public good", *Artificial Intelligence and Law* 22, 2: 113-139.

Lamport, Leslie and Robert Shostak & Marshall Pease. (1982). "The Byzantine Generals Problem", *ACM Transactions on Programming Languages and Systems*, *4*(3), 382-401.

Lawson, Brian (2013). “Individual Complicity in Collective Wrongdoing” *Ethical Theory and Moral Practice* 16 (2): 227–43.
Lewis, David (1970). “How to Define Theoretical Terms”, *Journal of Philosophy*, 67: 427–446.
Li, Aya and Xianhua Wei & Zhou He (2020). “Robust Proof of Stake: A New Consensus Protocol for Sustainable Blockchain Systems” *Sustainability* 12, 2844: 1-15.
Li, Feng and Bruce McMillin (2014). “A Survey on Zero-Knowledge Proofs" *Advances in Computers* 94: 25-69. https://doi.org/10.1016/B978-0-12-800161-5.00002-5
Lopp, Jameson (2018). “Who Controls Bitcoin Core?’” Blog post. Available online: https://blog.lopp.net/who-controls-bitcoin-core-/
Lopp, Jameson (2019). “Thoughts on Libra ‘Blockchain’” Blog post. Available online: https://blog.lopp.net/thoughts-on-libra--blockchain-/
Lopp, Jameson (2020). “Bitcoin Information & Educational Resources”. Available online: https://www.lopp.net/bitcoin-information.html
Luther, William J. (2013). "Friedman versus Hayek on Private Outside Monies: New Evidence for the Debate" *Economic Affairs* 33, 1: 127-135.
Luther, William J. (2016a). "Cryptocurrencies, Network Effects, and Switching Costs" *Contemporary Economic Policy* 34, 3: 553–571.
Luther, William J. (2016b). "Bitcoin and the Future of Digital Payments" *The Independent Review* 20, 3: 397-404.
Luther, William J. (2018a). “In Defense of Cash” *Reason Magazine* May 2018: 36-41.
Luther, William J. (2018b). “Getting off the ground: the case of bitcoin” *Journal of Institutional Economics* 15, 2: 189-205.
Luther, William J. (2018c). “Is Bitcoin intrinsically worthless?” *The Journal of Private Enterprise* 33, 1: 31-45.
Luther, William J. (2020). “Regulatory ambiguity in the market for bitcoin” *Review of Austrian Economics*. https://doi.org/10.1007/s11138-019-00489-2
Luther, William J. and Sean Stein Smith (2020). “Is Bitcoin a decentralized payment mechanism?” *Journal of Institutional Economics* 16: 433-444.
Mafi-Kreft, Elham (2003). "The Relationship Between Currency Competition and Inflation" *Kyklos* 56, 4: 475–490.
McIntyre, Alison (2019). "Doctrine of Double Effect", *The Stanford Encyclopedia of Philosophy*, Edward N. Zalta (ed.), URL = <https://plato.stanford.edu/archives/spr2019/entries/double-effect/>.
Malcolm, Jeremy (2017). "Payment Processors are Still Policing Your Sex Life, and the Latest Victim is FetLife" Electronic Frontier Foundation. Available online: https://www.eff.org/deeplinks/2017/03/payment-processors-are-still-policing-your-sex-life
Malherbe, Léo and Matthieu Montalban, Nicolas Bédu & Caroline Granier (2019). Cryptocurrencies and Blockchain: Opportunities and Limits of a New Monetary Regime" *International Journal of Political Economy* 48, 2: 127-152.
Mann, Ronald J. and Seth R. Belzley (2005). "The Promise of Intermediary Liability" 47 Wm. & Mary L. Rev. 239, 280.

Martin, Antoine and Stacey Schreft (2006). "Currency competition: A partial vindication of Hayek" *Journal of Monetary Economics* 53: 2085-2111.

Matsakis, Louise (2019). "How the West Got China's Social Credit System Wrong" Wired Magazine. Available online: https://www.wired.com/story/china-social-credit-score-system/

Matthews, Steve (2010). "Anonymity and the Social Self" *American Philosophical Quarterly* 47, 4:351 - 363.

Maurer, Bill and Taylor C. Nelms & Lana Swartz (2013). "'When perhaps the real problem is money itself!': the practical materiality of Bitcoin" *Social Semiotics* 23, 2: 261-277.

McDonell, Stephen (2019). "China social media: WeChat and the Surveillance State". BBC News. Available online: https://www.bbc.com/news/blogs-china-blog-48552907

McDowell, Daniel. (2020a). Financial sanctions and political risk in the international currency system. *Review of International Political Economy*, 1-27.

McDowell, Daniel (2020b). "Payments Power: The Overlooked Role of the Dollar as the Top International Payments Currency" International Studies Perspectives 1–45, pp. 12-18.

Mitchell, Bruce and Juan Franco (2018). "HOLC "Redlining" Maps: The Persistent Structure Of Segregation And Economic Inequality" NCRC. Available online: https://ncrc.org/wp-content/uploads/dlm_uploads/2018/02/NCRC-Research-HOLC-10.pdf

Mooradian, Norman (2009). "The importance of privacy revisited" *Ethics and Information Technology* 11,3: 163-174.

Moore, Adam D. (2018). "Privacy, Interests, and Inalienable Rights" *Moral Philosophy and Politics* 5, 2:327-355.

Nakamoto, Satoshi (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System". Available online: https://bitcoin.org/bitcoin.pdf

Narayanan, Arvind, and Jeremy Clark (2017). "Bitcoin's academic pedigree." *Communications of the ACM* 60.12 : 36-45.

Nisbet, Eric C. and Elizabeth Stoycheff & Katy E. Pearce (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.

Norland, Eric and Blu Putnam (2019). Bitcoin Economics in *Economics Gone Astray* (Putnam, Norland, and Arasu, eds.), 81-94. World Scientific Publishing Co.

OpenStax (2020). Principles of Macroeconomics (open-source textbook). Available online: http://cnx.org/contents/4061c832-098e-4b3c-a1d9-7eb593a2cb31@10.49:2/Macroeconomics

O'Sullivan, Andrea (2018). "Ungoverned or Anti-Governance? How Bitcoin Threatens the Future of Western Institutions" *RIPE series in global political economy* 71, 2: 90-102

Parino, Francesco, Mariano G. Beiró, and Laetitia Gauvin (2018). "Analysis of the Bitcoin blockchain: socio-economic factors behind the adoption" *EPJ Data Science* 7:38: 1-23.

Pease, Marshall and Robert Shostak & Leslie Lamport. (1980). "Reaching Agreement in the Presence of Faults. *Journal of the ACM (JACM)*, *27*(2), 228-234.

Pew (2012). "Payday Lending in America: Who Borrows,Where They Borrow, and Why", Pew Charitable Trusts. Available online:

https://www.pewtrusts.org/-/media/legacy/uploadedfiles/pcs_assets/2012/pewpaydaylendingreportpdf.pdf
Pickel, Andreas (1989). "Never Ask Who Should Rule: Karl Popper and Political Theory", *Canadian Journal of Political Science* Vol. 22,1: 83-105.
Pillay, Jeevan (2020). "Quadratic Proof of Stake" Blog post. Available online: https://ethresear.ch/t/quadratic-proof-of-stake-qpos/6842
Poelstra, Andrew (2015). "On Stake and Consensus". Available online: https://www.lopp.net/pdf/On-Stake-and-Consensus.pdf
Rachels, James (1975). "Why privacy is important" *Philosophy and Public Affairs* 4, 4: 323-333.
Racsko, Peter (2019). "Blockchain and Democracy" *Society and Economy* 41: 353-369.
Rahman, Adib (2018). "Deflationary policy under digital and fiat currency competition" *Research in Economics* 72: 171–180.
Rahn, Richard (1999). *The End of Money and the Struggle for Financial Privacy*. The Discovery Institute.
Reid, Fergal and Martin Harrigan (2012). "An Analysis of Anonymity in the Bitcoin System" *Security and Privacy in Social Networks* (Altshuler, Elovici, Cremers, Aharony, and Pentland, eds): 197-223.
Reitman, Rainey (2012). "Legal Censorship: PayPal Makes a Habit of Deciding What Users Can Read". Electronic Frontier Foundation. Available online: https://www.eff.org/deeplinks/2012/02/legal-censorship-paypal-makes-habit-deciding-what-users-can-read
Rogoff, Kenneth S. (2016). *The Curse of Cash*. Princeton University Press.
Rosenbaum, Kalle. (2019). *Grokking Bitcoin*. Shelter Island: Manning.
Rössler, Beate (2005). *The Value of Privacy*. Polity Press.
Rothstein, Richard (2018). *The Color of Law: A Forgotten History of How Our Government Segregated America*. New York: Liveright.
Ruijgrok, Kris (2017). "From the web to the streets: internet and protests under authoritarian regimes." *Democratization* 24, 3: 498-520.
Salter, Alexander W and William J. Luther (2019). "Adaptation and central banking" *Public Choice* 180: 243-256.
Samuelson, Paul A. and William D. Nordhaus (2010). *Economics* (19th ed). Boston: McGraw-Hill.
Shiller, Robert (1997). "Why Do People Dislike Inflation?" in *Reducing Inflation* (Romer and Romer, eds), 13-70. Chicago: Chicago University Press.
Selgin, George A. and Lawrence H. White (1994). "How Would the Invisible Hand Handle Money?" *Journal of Economic Literature* 32: 1718-1749.
Selgin, George A. (2015). "Synthetic Commodity Money." *Journal of Financial Stability* 17: 92–99.
Shilling, Linda and Harald Uhlig (2019). "Some simple bitcoin economics". *Journal of Monetary Economics* 106: 16-26.
Smit, J.P and Filip Buerens and Stan Du Plessis (2016). "Cigarettes, dollars and bitcoins – an essay on the ontology of money" *Journal of Institutional Economics* 12, 2: 327–347.
Song, Jimmy (2019). *Programming Bitcoin*. Boston: O'Reilly.

Stoycheff, Elizabeth, and Erik C. Nisbet (2014). "What's the bandwidth for democracy? Deconstructing Internet penetration and citizen attitudes about governance." *Political Communication* 31, 4: 628-646;

SWIFT (2015). "Worldwide Currency Usage and Trends." SWIFT Information Paper. Available online: https://www.swift.com/sites/default/files/documents/swift_bi_currency_evolution_infopaper_57128.pdf

Swire, Peter P. (1999). "Financial Privacy and the Theory of High-Tech Government Surveillance" 77 Wash. U. L. Q. 461.

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

Tusikov, Natasha (2016). *Chokepoints: Global Private Regulation of the Internet*. University of California Press.

Tusikov, Natasha (2019). "Defunding Hate: PayPal's Regulation of Hate Groups." *Surveillance & Society* 17.1/2: 46-53.

van den Hoven, Jeroen, Blaauw, Martijn, Pieters, Wolter and Warnier, Martijn (2020). "Privacy and Information Technology", *The Stanford Encyclopedia of Philosophy* (Summer 2020 Edition), Edward N. Zalta (ed.), URL = <https://plato.stanford.edu/archives/sum2020/entries/it-privacy/>.

Véliz, Carissa (2019). "The Internet and Privacy" In David Edmonds (ed.), *Ethics and the Contemporary World*, 149-159. Routledge.

Vincent, Danny (2016). "We looked inside a secret Chinese bitcoin mine". BBC Future. Available online: https://www.bbc.com/future/article/20160504-we-looked-inside-a-secret-chinese-bitcoin-mine

Walch, Angela (2015). "The bitcoin blockchain as financial market infrastructure: consideration of operational risk" *New York University Journal of Legislation and Public Policy* 18, 4: 837-894.

Walch, Angela (2018). "Blockchain Applications to International Affairs: Reasons for Skepticism". *Georgetown Journal of International Affairs*, 19: 27-35.

Walch, Angela (2019). "Decentralization': Exploring the Core Claim of Crypto Systems" in *Cryptoassets: Legal, Regulatory, and Monetary Perspectives* (Brummer, ed.). Oxford: Oxford University Press.

Warmke, Craig (manuscript a). "Electronic coins."

Warmke, Craig (manuscript b). "What is Bitcoin?"

West, Sarah Myers (2019). "Data capitalism: Redefining the logics of surveillance and privacy." *Business & Society* 58.1: 20-41.

Wigoder, Natasha (2019). "Inside China's Massive Surveillance Operation" Wired Magazine. Available online: https://www.wired.com/story/inside-chinas-massive-surveillance-operation/

World Bank (2020). "Remittance Prices Worldwide". Available online: https://remittanceprices.worldbank.org/en

Yermack, David (2015). “Is Bitcoin a Real Currency?” In David K.C. Lee ed., *The Handbook of Digital Currency*, 31-44. Elsevier.

Zahnentferner, Joachim (2018). "Chimeric Ledgers: Translating and Unifying UTXO-based and Account-based Cryptocurrencies." *IACR Cryptol. ePrint Arch*: 262.

Zelmanovitz, Leonidas (2016). *The Ontology and Function of Money: The Philosophical Fundamentals of Monetary Institutions*. London: Lexington Books.

Zuboff, Shoshana (2019). *The age of surveillance capitalism: the fight for the future at the new frontier of power*. London: Profile Books.